

Steinberg lattice of the general linear group and its modular reduction

FERNANDO SZECHTMAN

1 Introduction

Let $G = \mathrm{GL}_n(q)$ be the general linear group of degree $n \geq 2$ defined over a finite field F_q of characteristic p . We fix a prime $\ell \neq p$ and let R denote a local principal ideal domain having characteristic 0, maximal ideal ℓR , and containing a primitive p -th root of unity. Then the residue field $K = R/\ell R$ has characteristic ℓ and a primitive p -th root of unity.

By a Steinberg lattice of G over R we understand a left RG -module, say M , which is free of rank $q^{n(n-1)/2}$ as an R -module and affords the Steinberg character. The reduction of M modulo ℓ is the KG -module $M/\ell M$.

In this paper *the* Steinberg lattice is the left ideal $I = RG \cdot \varepsilon$ of the group algebra RG ,

$$\varepsilon = \sum_{\sigma \in S_n} \mathrm{sg}(\sigma) \sigma \hat{B}, \quad (1)$$

where the symmetric group S_n is viewed as a subgroup of G , we let B denote the upper triangular group, and $\hat{S} = \sum_{s \in S} s$ for any subset S of G .

Our main object of study is the ℓ -modular reduction of I , namely the KG -module $L = I/\ell I$. In particular, we wish to find a composition series of L , the socle and radical series of L , the length, say $c(L)$, of L , and any additional structural information about I and L that might be of use in achieving these goals, or interesting in its own right.

Many other Steinberg lattices and their corresponding reductions modulo ℓ appear in a natural manner, and will be compared to I and L .

The first results are due to Steinberg [5]. Let U be the upper unitriangular group, i.e. the Sylow p -subgroup of B . Then I is a free R -module with basis $\{u\varepsilon \mid u \in U\}$ and U acts on I via the regular representation. Naturally L has K -basis $\{u \cdot (\varepsilon + \ell I) \mid u \in U\}$ and affords the regular representation of U . Moreover, L is irreducible if and only if $\ell \nmid [G : B]$. Steinberg did not state it explicitly, but it is obvious from [5] that the socle of L , say $\mathrm{soc}(L)$, is irreducible.

There is a canonical symmetric bilinear form $RG \times RG \rightarrow R$ given by $(g, h) \mapsto \delta_{g,h}$. Restriction to I followed by scaling by $1/|B|$ yields the G -invariant symmetric bilinear form $f : I \times I \rightarrow R$ with zero radical studied by Gow in [4]. He uses f to produce the RG -submodules $I(c)$ of I given by

$$I(c) = \{x \in I \mid f(x, I) \subseteq \ell^c R\}, \quad c \geq 0.$$

This yields the following filtration of RG -modules, where all inclusions are strict:

$$I = I(0) \supset I(1) \supset I(2) \supset \cdots . \quad (2)$$

He next considers the KG -submodules $L(c)$ of L defined by

$$L(c) = (I(c) + \ell I) / \ell I, \quad c \geq 0,$$

which give rise to a filtration of KG -modules

$$L = L(0) \supseteq L(1) \supseteq L(2) \supseteq \cdots . \quad (3)$$

Each factor of (3) is a KG -module and will be denoted by

$$M(c) = L(c) / L(c+1), \quad c \geq 0.$$

As L is finite dimensional, the series (3) must eventually stabilize and there may be prior repetitions. The question as to when exactly this happens was settled by Gow. Write \mathcal{P} for the lattice of standard parabolic subgroups of G , i.e. those containing B . A non-negative integer c is said to be a \mathcal{P} -value if $\ell^c \mid [G : P]$ but $\ell^{c+1} \nmid [G : P]$, i.e. $\nu_\ell([G : P]) = c$, for some $P \in \mathcal{P}$. Let V stand for the total number of \mathcal{P} -values. Gow proves that the factor $M(c)$ is non-zero if and only if c is a \mathcal{P} -value. Furthermore, if $b = \nu_\ell([G : P])$, the largest \mathcal{P} -value, then $L(b) = \text{soc}(L)$, which by above is irreducible. Since $L(b)/L(b+1) \neq 0$, it follows that $0 = L(b+1) = L(b+2) = \cdots$.

Clearly Gow's work implies $c(L) \geq V$, with equality if and only if $M(c)$ irreducible for every \mathcal{P} -value c , that is, if and only if (3) is a composition series of L . All repeated terms in (3) must be deleted when interpreting this statement. Looking at the last line of

the decomposition matrices for unipotent representations of $\mathrm{GL}(n, q)$, $n \leq 10$, as given by James in [3], Gow believed that $c(L) = V$ and conjectured this would hold for any n .

Let

$$e = \min\{i \geq 2 \mid \ell \text{ divides } \frac{q^i - 1}{q - 1}\},$$

and note that if $\ell \nmid q - 1$ then e divides $\ell - 1$ and is the order of q modulo ℓ , while if $\ell \mid q - 1$ then $e = \ell$.

Gow's observation is based on the matrices explicitly displayed in [3], which equal the decomposition matrices as long as $\lfloor n/e \rfloor < \ell$. To obtain the latter when $\lfloor n/e \rfloor \geq \ell$ requires adjustment matrices, as indicated by James. We will come back to this point shortly.

As long as $\lfloor n/e \rfloor < \ell$, Gow's conjecture does hold for any n , as shown by Ackermann (see Section 4.6 of [1]), who proved, among many other things, that L is uniserial of length $c(L) = V = \lfloor n/e \rfloor + 1$, provided $\lfloor n/e \rfloor < \ell$. Furthermore, Theorem 8.1 verifies Gow's conjecture in many other cases, including the case $\lfloor n/e \rfloor \leq \ell$, and Theorem 6.1 proves that if $\lfloor n/e \rfloor > \ell$ then the first $\ell + 1$ non-zero factors of (3), starting at the bottom, are indeed irreducible. In addition, Theorem 4.10 proves that the top factor $M(0) = L(0)/L(1)$ is irreducible under no restrictions at all. Moreover, we know from [6] that $M(c)$ is a completely reducible KG -module. Furthermore, Sections 2 and 3 associate a non-zero cyclic submodule $N(P)$ of $M(c)$ to any $P \in \mathcal{P}(c)$ and prove it to be irreducible.

In spite of all this evidence Gow's conjecture is actually false. Indeed, for $c \geq 0$ let $\mathcal{P}(c)$ consist of all $P \in \mathcal{P}$ such that $\nu_\ell([G : P]) = c$. Let \mathcal{P}^* be the set of all standard parabolic subgroups that correspond to partitions of n where every part is either 1 or of the form $e\ell^i$ for some $i \geq 0$. Define $\mathcal{P}^*(c) = \mathcal{P}(c) \cap \mathcal{P}^*$. Section 4 shows that $M(c)$ equals the direct sum of all distinct $N(P)$ as P runs through $\mathcal{P}^*(c)$. Thus, Gow's conjecture translates as follows: the $N(P)$ are all *equal*, $P \in \mathcal{P}^*(c)$, whenever c is a \mathcal{P} -value. We tried very hard to prove this, without success. Then, together with D. Djokovic, we examined James' tables and noticed that the correct decomposition matrices for $n \leq 10$ give $c(L) = |\mathcal{P}^*|$, which is equivalent to the $N(P)$ being *distinct* for all $P \in \mathcal{P}(c)$ and all \mathcal{P} -values c , i.e. a composition series of L is obtained by refining (3) by means of the decomposition

$$M(c) = \bigoplus_{P \in \mathcal{P}^*(c)} N(P). \quad (4)$$

Here in general $|\mathcal{P}^*(c)| \neq 1$. In particular L is not always uniserial. This paper does not study whether $c(L) = |\mathcal{P}^*|$, and hence (4), hold for all n . As illustration we refer the reader to Examples 9.1 and 9.2.

Let us turn to the contents of the paper. Section 2 contains definitions and notation, as well as basic facts about I and L to be used throughout the article. It also defines $N(P)$, whose irreducibility is proven in Section 3. Section 4 associates to every $P \in \mathcal{P}(c)$ a suitable $P^* \in \mathcal{P}^*(c)$ satisfying $N(P^*) = N(P)$, explicitly computes the common value $\nu_\ell([P : B]) = \nu_\ell([P^* : B])$, and shows that $M(c)$ is the direct sum of all distinct $N(P^*)$ as P^* runs through $\mathcal{P}^*(c)$. These proofs are long. To not interrupt the flow of the paper we created Appendix A to deal with the transfer of information from the lattice \mathcal{P} of standard parabolic subgroups to the Steinberg lattice I and hence to its modular reduction L , and Appendix B to develop the auxiliary tools to find the exact value of $\nu_\ell([P : B])$.

Section 4 also proves that the top factor $M(0) = L(0)/L(1)$ is irreducible, where $L(1)$ is the only maximal submodule of L , i.e. $\text{rad}(L) = L(1)$. This result is dual to the aforementioned fact that $M(b) = L(b) = \text{soc}(L)$ is irreducible. That this is not to be taken for granted is shown by Examples 5.4 and 5.5 of [4], where the reduction modulo ℓ of the Steinberg lattice of $\text{Sp}(4, q)$ is seen not to be irreducible modulo its radical.

We spend considerable effort -see Theorems 6.5 and 6.7- demonstrating that the socle and radical series of L simply agree with (3), provided the positive integer

$$d = \nu_\ell\left(\frac{q^e - 1}{q - 1}\right) \tag{5}$$

is equal to one. This is a pleasant state of affairs taking into account how differently these series are defined and the fact that L in general is not uniserial, even when $d = 1$. We do not know if Theorems 6.5 and 6.7 hold when $d > 1$.

Regarding $c(L)$, we know from above that $V \leq c(L) \leq |\mathcal{P}^*|$. Under strong hypotheses, such as in Theorem 8.5, all three of these numbers coincide. In general, we have a recursive formula for $|\mathcal{P}^*|$ (Lemma 8.4) and an explicit one for V (Theorem 6.3). In most cases V is a polynomial in ℓ which depends on d and the digits of $\lfloor n/e \rfloor$ when written in base ℓ .

Theorem 4.8 finds a new generator for I that is a common eigenvector when U acts on I . While the statement of our result makes sense for all finite groups of Lie type, it need

not hold outside of type A . Indeed, in Examples 5.4 and 5.5 of [4] we find that the top factor of the analogue of L for $\mathrm{Sp}(4, q)$ is completely reducible. If any common eigenvector for the action of U generated I , the top factor of L would be irreducible, against [4].

Theorem 5.3 computes the endomorphism ring of any term of the series (2) or (3): it consists entirely of scalar operators.

As noted in [4], each term $I(c)$ of (2) is free of rank $|U|$. It follows that $I(c)$ is a Steinberg lattice. Let $T^c = I(c)/\ell I(c)$ stand for the reduction of $I(c)$ modulo ℓ . In this notation, $L = T^0$. The KG -modules T^c are studied in Section 7. Surprisingly, they are pairwise non-isomorphic for all \mathcal{P} -values c . Consequently, the RG -modules $I(c)$, for all \mathcal{P} -values c , are non-isomorphic to each other. By a well-known theorem of Brauer and Nesbitt, the non-isomorphic KG -modules T^c must have the same composition factors. We obtain a direct proof of this fact by comparing the factors of the series (2) and (3). We also find that the socle of T^c , $0 < c < b$, is no longer irreducible, as it contains copies of $M(b) = L(b)$ and $M(0)$. This contrasts with the cases of L and $T^b \cong L^*$, both of which have an irreducible socle. We wonder if there is a Steinberg lattice whose reduction modulo ℓ is completely reducible for $\ell \mid [G : B]$.

Finally, we investigate when $|\mathcal{P}^*(c)| = 1$ for all \mathcal{P} -values c , which, by above, is a sufficient condition for (3) to be a composition series of L . The answer, Theorem 8.1, depends on various cases and will not be stated here. Its case by case proof is given in Appendix C. In any case, (3) is a composition series of L if $\lfloor n/e \rfloor \leq \ell$. The bottom $\ell + 1$ non-zero factors of (3) remain irreducible if $\lfloor n/e \rfloor > \ell$ (Theorem 6.1).

2 Preliminaries

Let e_1, \dots, e_n be the canonical basis of the column space F_q^n . For $\sigma \in S_n$ we have the permutation matrix $\tilde{\sigma} \in G$ given by $\tilde{\sigma}e_i = e_{\sigma(i)}$. We abuse notation and identify σ with $\tilde{\sigma}$.

Let Π be the set of all fundamental transpositions $(1, 2), \dots, (n-1, n)$. There is a natural bijection from the set of all subsets of Π onto \mathcal{P} , given by $J \mapsto P_J = \langle B, J \rangle$.

To any (i, j) , with $1 \leq i \neq j \leq n$, there corresponds the root subgroup X_{ij} of G formed by all matrices $t_{ij}(a) = I_n + aE^{ij}$, as a runs through F_q .

Let R^* stand for the unit group of R . To a group homomorphism $\lambda : U \rightarrow R^*$ we associate the set $J(\lambda) \subseteq \Pi$ of all $(i, i+1)$ such that λ is non-trivial on $X_{i,i+1}$ and let

$$P(\lambda) = P_{J(\lambda)}$$

be the corresponding standard parabolic subgroup. Every $P \in \mathcal{P}$ arises in this way.

2.1 $M(c) \neq 0$ for every \mathcal{P} -value c

Fix a group homomorphism $\lambda : U \rightarrow R^*$ and let $P = \mathcal{P}(\lambda) \in \mathcal{P}$, $c = \nu_\ell([G : P])$. Associated to λ we have the element E_λ of I defined by

$$E_\lambda = \sum_{u \in U} \lambda(u) u \varepsilon \in I. \quad (6)$$

We see U acts on E_λ via λ^{-1} and any $x \in I$ with this property is a scalar multiple of E_λ .

Let f be the bilinear form on I defined in the Introduction. As seen in Section 3 of [4]

$$f(E_\lambda, u \varepsilon) = \lambda(u)[G : P], \quad u \in U. \quad (7)$$

It follows that

$$E_\lambda \in I(c) \quad (8)$$

and

$$E_\lambda \notin I(c+1). \quad (9)$$

Let

$$F_\lambda = E_\lambda + \ell I \in L.$$

We see from above that

$$F_\lambda \in L(c). \quad (10)$$

It was asserted in Section 4 of [4] that

$$F_\lambda \notin L(c+1). \quad (11)$$

This does not follow automatically from (9), and we pause to verify this crucial assertion.

We need to show that $E_\lambda \notin I(c+1) + \ell I$. Since $P(\lambda) = P(\lambda^{-1})$ we have $E_{\lambda^{-1}} \in I(c)$, as

above. Therefore, for all $x \in I(c+1) + \ell I$

$$f(x, E_{\lambda-1}) \in \ell^{c+1}R.$$

But (7) gives

$$f(E_\lambda, E_{\lambda-1}) = |U|[G : P(\lambda)],$$

where $\ell \nmid |U|$, so indeed $E_\lambda \notin I(c+1) + \ell I$, as claimed. Combining (11) and (10) we obtain

2.1 Theorem (Gow) The KG -module $M(c) = L(c)/L(c+1) \neq 0$ for every \mathcal{P} -value c .

Since $F_\lambda \in L(c)$ but $F_\lambda \notin L(c+1)$ we see that

$$N(\lambda) = KG \cdot (F_\lambda + L(c+1)). \quad (12)$$

is a non-zero cyclic submodule of $M(c)$. We will see shortly that $N(\lambda)$ is irreducible.

2.2 $M(c) \neq 0$ implies that c is a \mathcal{P} -value

To derive the converse of Theorem 2.1 we require two further tools. The first, taken from [6], was originally proven by Gelfand and Graev for complex representations.

2.2 Theorem A non-zero KG -module has a one dimensional U -invariant subspace.

2.3 Lemma The natural group homomorphism $\lambda \mapsto \bar{\lambda}$, where $\bar{\lambda}(u) = \lambda(u) + \ell R$, from the group of all group homomorphisms $U \rightarrow R^*$ to the group of all group homomorphisms $U \rightarrow K^*$, is an isomorphism.

Proof. Since U/U' is an elementary abelian p -group and both R^* and K^* possess a non-trivial p -root of unity, we see that the groups our map is connecting have the same size, namely $|U/U'|$. It thus suffices to show that our map is injective. For this purpose, suppose that $\bar{\lambda}$ is trivial. We wish to show that λ must be trivial. If not, then $\lambda(u) = a \neq 1$ for some $u \in U$. As $\bar{\lambda}$ is trivial, $x = a - 1 \in \ell R$. Thus $a = 1 + x$ is a p -root of unity with $x \neq 0$ in ℓR . Let $k \geq 1$ be the ℓ -valuation of x . Then the ℓ -valuation of x^p is $kp > k$. But

$$1 = a^p = (1 + x)^p = 1 + px + \cdots + px^{p-1} + x^p.$$

Subtracting 1 from each side yields $x^p = -px(1+c)$, where $c \in \ell R$. Since p and $1+c$ are units in R , we reach the contradiction that the ℓ -valuation of x^p is k .

2.4 Proposition Let $c \geq 0$ be arbitrary and let M be a KG -submodule of L properly containing $L(c+1)$. Then M contains F_λ for some group homomorphism $\lambda : U \rightarrow R^*$ such that $k = \nu_\ell([G : P(\lambda)]) \leq c$. If actually $M \subseteq L(c)$ then $k = c$.

Proof. By assumption $M/L(c+1)$ is a non-zero KG -module. Then $M/L(c+1)$ has a one dimensional U -invariant subspace, say $A/L(c+1)$, where A is a KU -submodule of M , by Theorem 2.2. Since $\ell \nmid |U|$, A is completely reducible as a KU -module. Let N be a KU -complement to $L(c+1)$ in A . Then N is a one dimensional KU -submodule of M not contained in $L(c+1)$.

Now U acts on N via a linear character, say $\mu : U \rightarrow K^*$. From Lemma 2.3 we know that $\mu = \bar{\eta}$ for a unique linear character $\eta : U \rightarrow R^*$. Let $\lambda = \eta^{-1}$. We easily see that U acts on F_λ via μ . Since U acts on L via the regular representation, it follows that $N = K \cdot F_\lambda$. Thus F_λ is in M but not in $L(c+1)$.

Suppose, if possible, that $k > c$. Then $k \geq c+1$, so $L(k) \subseteq L(c+1)$. But $F_\lambda \in L(k)$ by (10), so $F_\lambda \in L(c+1)$, a contradiction. This proves the first assertion.

Assume next that $M \subseteq L(c)$. Suppose, if possible, that $k < c$. Then $k+1 \leq c$ so $F_\lambda \in M \subseteq L(c) \subseteq L(k+1)$, against (11). This completes the proof.

Proposition 2.4 applied to $M = L(c)$ yields

2.5 Theorem (Gow) If the KG -module $M(c) = L(c)/L(c+1) \neq 0$ then c is a \mathcal{P} -value.

2.3 Notation associated to parabolic subgroups

Let H be the diagonal subgroup of G . As U is normalized by H we have an action of H on the set of all group homomorphisms $U \rightarrow R^*$. The orbits of this action are parametrized by \mathcal{P} . Indeed, the H -orbit of $\lambda : U \rightarrow R^*$ is formed by all $\mu : U \rightarrow R^*$ such that $P(\lambda) = P(\mu)$.

Fix $P \in \mathcal{P}$ for the remainder of this subsection and let $c = \nu_\ell([G : P])$.

Given a group homomorphism $\lambda : U \rightarrow R^*$ and $h \in H$ we see from (6) that

$$h \cdot E_\lambda = E_{h\lambda}, \quad h \in H.$$

If $\mu : U \rightarrow R^*$ is also group homomorphism and $P(\lambda) = P(\mu)$ we can then find h in H such that ${}^h\lambda = \mu$. We conclude that $RG \cdot E_\lambda = RG \cdot E_\mu$ whenever $P(\lambda) = P(\mu)$. We may thus define RG -submodule $I'(P)$ of I by

$$I'(P) = RG \cdot E_\lambda$$

for any λ such that $P(\lambda) = P$. We also define the KG -submodule $L'(P)$ of L by

$$L'(P) = (I'(P) + \ell I) / \ell I = KG \cdot F_\lambda$$

and the KG -submodule $N(P)$ of $M(c)$

$$N(P) = (L'(P) + L(c+1)) / L(c+1) = KG \cdot (F_\lambda + L(c+1)) = N(\lambda)$$

for any choice of λ satisfying $P(\lambda) = P$. We further define

$$I(P) = I(c), \quad L(P) = L(c), \quad M(P) = M(c).$$

In this notation, we have the following result.

2.6 Corollary Eliminating repeated terms from (3) produces (all inclusions are proper):

$$0 \subset L(P_0) \subset \cdots \subset L(P_{V-1}) = L, \tag{13}$$

where $P_0, \dots, P_{V-1} \in \mathcal{P}$ are chosen so that $\nu_\ell([G : P_0]) > \cdots > \nu_\ell([G : P_{V-1}])$.

We find it useful to have a notation to pass from one term of (13) to the next. Let

$$L(P)^\sharp = L(c+1).$$

Thus $L(P)^\sharp = 0$ if $c = b$ and $L(P)^\sharp = L(Q)$ if $\nu_\ell([G : Q])$ is the first \mathcal{P} -value larger than c .

3 Irreducibility of $N(\lambda)$

We quote the following result from [6].

3.1 Theorem $M(c)$ is completely reducible and self-dual, while L is multiplicity free.

3.2 Theorem Let $\lambda : U \rightarrow R^*$ be a group homomorphism with $c = \nu_\ell([G : P(\lambda)])$. Then $N(\lambda)$, as defined in (12), is an absolutely irreducible KG -sumodule of $M(c)$.

Proof. We know from Theorem 3.1 that $M(c)$, and hence $N(\lambda)$, is completely reducible, so it suffices to show that the only KG -endomorphisms of $N(\lambda)$ are scalars.

Let $\mu : U \rightarrow K^*$ be the group homomorphism corresponding to $\lambda^{-1} : U \rightarrow R^*$ by the natural projection $R^* \rightarrow K^*$. Since U acts on L via the regular representation and $\ell \nmid |U|$ we see that μ enters a given KU -section of L at most once. But construction, if $x = F_\lambda + L(c+1)$, then $u \cdot x = \mu(u)x$ for all $u \in U$. Moreover, $0 \neq x \in N(\lambda)$ shown in Section 2. It follows that the subspace of $N(\lambda)$ where U acts via μ is one dimensional and spanned by x . Let α be an arbitrary KG -endomorphism of $N(\lambda)$. If $u \in U$ then

$$u\alpha(x) = \alpha(ux) = \alpha(\mu(u)x) = \mu(u)\alpha(x),$$

whence $\alpha(x) = ax$ for some $a \in K$ by above. But $N(\lambda) = KGx$ by construction, so if $y \in N(\lambda)$ then $y = rx$ for some $r \in KG$, whence $\alpha(y) = ay$, as required.

3.3 Corollary Let c be a \mathcal{P} -value. Then every irreducible submodule of $M(c)$ must be of the form $N(\lambda)$ for some $\lambda : U \rightarrow R^*$ satisfying $c = \nu_\ell([G : P(\lambda)])$.

Proof. This follows from Proposition 2.4.

3.4 Corollary All irreducible constituents of L are absolutely irreducible.

Proof. Using the series (3), this follows from Theorem 3.1 and Corollary 3.3.

4 Construction of \mathcal{P}^* and first consequences

A composition of n is a sequence (a_1, \dots, a_k) such that a_1, \dots, a_k are positive integers adding up to n . There is a natural bijection from the set of all compositions of n onto \mathcal{P} , given by $(a_1, \dots, a_k) \mapsto P_{(a_1, \dots, a_k)}$, the block upper triangular group with blocks of sizes a_1, \dots, a_k . By abuse of notation we will identify each $P \in \mathcal{P}$ with its corresponding composition.

A parabolic subgroup $Q = (b_1, \dots, b_l)$ is equivalent to P if $k = l$ and (b_1, \dots, b_k) is a rearrangement of (a_1, \dots, a_k) . Thus, the parabolic subgroups equivalent to P can be obtained by repeated application of single swaps of the form $a_i \leftrightarrow a_{i+1}$.

4.1 Theorem If $Q \in \mathcal{P}$ is equivalent to a subgroup of $P \in \mathcal{P}$ then $I'(Q) \subseteq I'(P)$ and, consequently, $L'(Q) \subseteq L'(P)$.

Proof. This can be found in Appendix A.

4.2 Corollary If P and Q are standard parabolic subgroups, $\nu_\ell([G : P]) = \nu_\ell([G : Q])$, and Q is equivalent to a subgroup of P , then $N(Q) = N(P)$.

Proof. This follows from Theorems 3.2 and 4.1.

Let

$$m = \max\{i \geq 0 \mid \ell^i \leq \lfloor n/e \rfloor\}.$$

Given $1 \leq a \leq n$ we write

$$\Delta(a) = (y_{-1}, y_0, \dots, y_m),$$

where $0 \leq y_{-1} < e$, $0 \leq y_i < \ell$ for $1 \leq i \leq m$, and $a = y_{-1} + e(y_0 + y_1\ell + \dots + y_m\ell^m)$. Thus y_{-1} is the remainder of dividing a by e and $(y_m \dots y_0)_\ell$ is the representation of $\lfloor a/e \rfloor$ in base ℓ . Given $P = (a_1, \dots, a_k) \in \mathcal{P}$ we let

$$\Delta(P) = \Delta(a_1) + \dots + \Delta(a_k).$$

Thus $\Delta(P) = (z_{-1}, z_0, \dots, z_m)$ is a sequence non-negative integers satisfying

$$z_{-1} + z_0e + z_1e\ell + \dots + z_me\ell^m = n.$$

We define

$$P^* = (\underbrace{1, \dots, 1}_{z_{-1}}, \underbrace{e, \dots, e}_{z_0}, \underbrace{e\ell, \dots, e\ell}_{z_1}, \dots, \underbrace{e\ell^m, \dots, e\ell^m}_{z_m}) = [z_{-1}, z_0, \dots, z_m]. \quad (14)$$

Let \mathcal{P}^* be set of all standard parabolic subgroups of the form (14). They correspond to partitions of n where each part is either 1 or of the form $e\ell^i$ for some $0 \leq i \leq m$.

Recall the definition (5) of d . We define the sequence s_0, s_1, \dots of positive integers by

$$s_0 = d, s_1 = \ell d + 1, s_2 = \ell^2 d + \ell + 1, s_3 = \ell^3 d + \ell^2 + \ell + 1, \dots$$

4.3 Theorem Let $P = (a_1, \dots, a_k) \in \mathcal{P}$. Then P^* , as defined in (14), is equivalent to a parabolic subgroup contained in P . Moreover,

$$\nu_\ell([P : B]) = s_0 z_0 + \dots + s_m z_m = \nu_\ell([P^* : B]) \text{ and } N(P) = N(P^*).$$

Proof. The very construction of P^* yields the first assertion. It is known and easy to see that

$$[P : B] = \prod_{1 \leq i \leq k} \prod_{1 \leq j \leq a_i} (q^j - 1) / (q - 1).$$

Let us write $\Delta(a_i) = (y_{-1}^i, y_0^i, \dots, y_m^i)$. Then by Lemma 11.5 of Appendix B we have

$$\nu_\ell([P : B]) = \sum_{1 \leq i \leq k} \nu_\ell \left(\prod_{1 \leq j \leq a_i} (q^j - 1) / (q - 1) \right) = \sum_{1 \leq i \leq k} (y_m^i s_m + \dots + y_0^i s_0) = z_m s_m + \dots + z_0 s_0.$$

As for P^* , the same argument (but using Lemma 11.3 of Appendix B instead) yields

$$\nu_\ell([P^* : B]) = \sum_{0 \leq i \leq m} z_i \times \nu_\ell \left(\prod_{1 \leq j \leq e \ell^i} (q^j - 1) / (q - 1) \right) = z_0 s_0 + \dots + z_m s_m.$$

This proves the second assertion. We may now derive the third from Corollary 4.2.

4.4 Corollary Let $[n/e] = (x_m \dots x_0)_\ell$. Then $b = \nu_\ell([G : B]) = s_0 x_0 + \dots + s_m x_m$.

4.5 Note Let $P \in \mathcal{P}$. Then P^* is the only member of \mathcal{P}^* that is equivalent to a standard parabolic subgroup contained in P and satisfies $\nu_\ell([P : B]) = \nu_\ell([P^* : B])$.

4.6 Theorem Let c be a \mathcal{P} -value. Then $M(c)$ has the following decomposition into non-isomorphic irreducible KG -modules:

$$M(c) = \oplus N(P),$$

where the sum runs through all different $N(P)$ produced by the $P \in \mathcal{P}^*(c)$.

Proof. This follows from Theorems 3.1, 3.2, 4.3 and Corollary 3.3.

4.7 Corollary $M(c)$ is irreducible if and only if c is a \mathcal{P} -value and $N(P) = N(Q)$ for all $P, Q \in \mathcal{P}^*(c)$. In particular, if $|\mathcal{P}^*(c)| = 1$ then $M(c)$ is irreducible, and if $|\mathcal{P}^*(c)| = 1$ for \mathcal{P} -values c then (3) is a composition series of L .

4.8 Theorem Let $\lambda : U \rightarrow R^*$ be a group homomorphism such that $P(\lambda) = G$, i.e. λ is non-trivial in every fundamental root subgroup. Then E_λ and F_λ , as defined in Section 2, respectively generate I and L , i.e. $I = RG \cdot E_\lambda$ and $L = KG \cdot F_\lambda$.

Proof. Let M the KG -submodule of L generated by the F_μ as μ runs through all group homomorphisms $U \rightarrow R^*$. By hypothesis $P(\mu) \subseteq P(\lambda)$ for every μ , so Theorem 4.1 gives $KG \cdot F_\lambda = M$. On the other hand, Theorem 2.2 and Lemma 2.3 show that $M = L$. Hence $KG \cdot F_\lambda = L$. Since the image of E_λ generates $L = I/\ell I$ and I is a finitely generated R -module, it follows from Nakayama's lemma that E_λ generates I .

4.9 Note If $P(\lambda) = G$ then Lemma 10.1 of Appendix A gives $E_\lambda = sg(\sigma_0) \sum_{u \in U} \lambda(u) u \sigma_0 \hat{B}$, where $\sigma_0 \in S_n$ is defined by $\sigma_0 = (1, n)(2, n-1)(3, n-2) \cdots$.

4.10 Theorem The top factor $M(0) = L(0)/L(1)$ of (3) is always irreducible.

Proof. $M(0) = N(G)$ by Theorem 4.8, so Theorem 3.2 applies.

4.11 Theorem All proper submodules of L are contained in $L(1)$, i.e. $rad(L) = L(1)$.

Proof. By above $L(1)$ is a maximal submodule of L . Suppose, if possible, that M is a proper submodule of L different from $L(1)$. Therefore $L(1) + M = L$, so by the second isomorphism theorem $L(1)/L(1) \cap M \cong (L(1) + M)/M = L/M$. Let λ be a linear character of U that is non-trivial in every fundamental root subgroup. As $L/L(1) \neq 0$ by Theorem 2.1 and $L/M \neq 0$ by assumption, Theorem 4.8 implies that λ enters both $L/L(1)$ and L/M . Hence λ enters both factors of the series $L \supset L(1) \supset L(1) \cap M$. This contradicts the fact that U acts on L via the regular representation with $\ell \nmid |U|$.

5 Endomorphism rings of $I(c)$ and $L(c)$

5.1 Lemma Every $L(P)$ is equal to the sum of the submodules $L'(Q)$ inside it.

Proof. This is certainly true for the irreducible module $L(B)$. Suppose that $\nu_\ell([P : B]) > 0$ and the statement is true $L(P)^\sharp$. Since $L(P)$ equals $L(P)^\sharp$ plus the sum of certain $L'(Q)$ inside $L(P)$ by Theorem 4.6, the result follows by induction.

5.2 Lemma Let $P \in \mathcal{P}$. Then the only endomorphisms of $L(P)$ are scalars.

Proof. Let f be an endomorphism of $L(P)$. Then f is determined by its values on the submodules $L'(Q)$ inside $L(P)$ by Lemma 5.1. Arguing as in the proof of Theorem 3.2 we see that if $\lambda : U \rightarrow K^*$ is any group homomorphism then $f(F_\lambda) = a(\lambda)F_\lambda$ for some $a(\lambda) \in K$. Let $\lambda_0 : U \rightarrow K^*$ be the trivial group homomorphism. Then F_{λ_0} belongs to all $KG \cdot F_\lambda$ by Theorem 4.1. It follows that all $a(\lambda)$ are equal to $a(\lambda_0)$, as required. (If $P = G$ we may use Theorem 4.8 to simplify the above argument.)

5.3 Theorem Each endomorphism of a term of the series (2) or (3) is a scalar.

Proof. Let F be the field of fractions of R . Then the Steinberg module $F \otimes_R I(c)$ over F is absolutely irreducible, so its only endomorphisms are scalars. It follows that the only endomorphisms of $I(c)$ are scalars. The case of $L(c)$ is given in Lemma 5.2.

5.4 Note Every $I(c)$ is generated as an RG -module by elements of form $\ell^i E_\lambda$.

Indeed, this is true for $I(0)$ by Theorem 4.8. Suppose $c > 0$ and the result is true for $I(c-1)$. Let N be the sum of all submodules $RG \cdot E_\lambda$ inside $I(c)$ and consider the KG -module $M = I(c)/(N + \ell I(c-1))$. We wish to show that $M = 0$. Consider the natural epimorphism $I(c) \rightarrow L(c)$. Its kernel is $I(c) \cap \ell I = \ell I(c-1)$. Thus $I(c)/\ell I(c-1) \cong L(c)$. Under this isomorphism $N + \ell I(c-1)/\ell I(c-1)$ corresponds to the submodule of $L(c)$ generated by all F_λ inside $L(c)$, namely $L(c)$, by Lemma 5.1. Thus

$$M/(N + \ell I(c-1)) \cong (I(c)/\ell I(c-1))/(N + \ell I(c-1)/\ell I(c)) \cong L(c)/L(c) = 0.$$

Therefore $M = N + \ell I(c-1)$, and the result follows by induction.

6 Socle and Radical series of L

For $P \in \mathcal{P}$ we set

$$\vartheta(P) = \nu_\ell([G : P]), \quad \phi(P) = \nu_\ell([P : B]).$$

Using $[G : B] = [G : P][P : B]$ and that V is the total number of \mathcal{P} -values we find that

$$|\{\vartheta(P) : P \in \mathcal{P}\}| = V = |\{\phi(P) : P \in \mathcal{P}\}|.$$

Recall that $e = \min\{i \geq 2 \mid \ell \text{ divides } \frac{q^i-1}{q-1}\}$ and set $m = \max\{i \geq 0 \mid \ell^i \leq \lfloor n/e \rfloor\}$. Let

$$\lfloor n/e \rfloor = (x_m \dots x_0)_\ell = x_m \ell^m + \dots + x_1 \ell + x_0.$$

Given nonnegative integers z_0, z_1, \dots, z_m satisfying $e(z_0 + \dots + z_m \ell^m) \leq n$ we set $z_{-1} = n - e(z_0 + z_1 \ell + \dots + z_m \ell^m)$ and reduce the notation $[z_{-1}, z_0, z_1, \dots, z_m]$ of (14) to $[z_0, z_1, \dots, z_m]$.

Thus,

$$[z_0, z_1, \dots, z_m] = (\underbrace{1, \dots, 1}_{z_{-1}}, \underbrace{e, \dots, e}_{z_0}, \underbrace{e\ell, \dots, e\ell}_{z_1}, \dots, \underbrace{e\ell^m, \dots, e\ell^m}_{z_m}) \in \mathcal{P}^*.$$

Recall also that $d = \nu_\ell(\frac{q^e-1}{q-1})$ and $b = \vartheta(B)$, whose exact value is given in Corollary 4.4.

We will also appeal to the notation introduced in Section 2.

6.1 Theorem (a) If $\lfloor n/e \rfloor \leq \ell$ then L is uniserial and its only composition series is (3).

(b) If $\lfloor n/e \rfloor > \ell$ then the first $\ell + 1$ terms of the socle series of L , together with 0, are $0 \subset L(P_0) \subset \dots \subset L(P_\ell)$, in the notation of Corollary 2.6. This is in fact a composition series of $L(P_\ell)$. In particular, $L(P_\ell)$ is uniserial of length $\ell + 1$ and the first $\ell + 1$ factors of (13) starting from the bottom are irreducible.

Proof. (a) Note that if $\lfloor n/e \rfloor < \ell$ then $\mathcal{P}^* = \{[i] \mid 0 \leq i \leq \lfloor n/e \rfloor\}$, while if $\lfloor n/e \rfloor = \ell$ then $\mathcal{P}^* = \{[i, 0] \mid 0 \leq i \leq \ell\} \cup \{[0, 1]\}$. In both cases \mathcal{P}^* is ordered by inclusion, which explains why L is uniserial.

Indeed, let us agree that the socle series of L starts at 0. Let $P \in \mathcal{P}^*$. Suppose that $L(P)^\sharp$ is equal to a term of the socle series of L and let S be the next term of this series. We wish to show that $S = L(P)$ with $S/L(P)^\sharp$ irreducible.

We have $L(P) \subseteq S$ by Theorem 3.1. Let M be a submodule of L properly containing $L(P)^\sharp$ with $M/L(P)^\sharp$ irreducible. We know from Proposition 2.4 that M contains $L'(Q)$ for some $Q \in \mathcal{P}^*$ satisfying $\vartheta(Q) \leq \vartheta(P)$. As \mathcal{P}^* is ordered by inclusion, $\vartheta(Q) \leq \vartheta(P)$ implies that P is contained in Q . This implies $L'(P) \subseteq L'(Q)$ by Theorem 4.1. Thus $M/L(P)^\sharp$ contains $N(P)$, so $M/L(P)^\sharp = N(P)$ by the irreducibility of $M/L(P)^\sharp$. As M was arbitrary, $S/L(P)^\sharp$ itself is irreducible and equal to $N(P)$. In particular, $S \subseteq L(P)$.

(b) Let $\mathcal{R} = \{[i, 0, \dots, 0] \mid 0 \leq i \leq \ell\}$. It is easy to see that if $P \in \mathcal{R}$, $Q \in \mathcal{P}^*$ and $\vartheta(Q) \leq \vartheta(P)$ then P is equivalent to a parabolic subgroup contained in Q . We may now

repeat the above proof with every $P \in \mathcal{R}$.

6.2 Corollary (a) If $\lfloor n/e \rfloor \leq \ell$ then $L(P) = L'(P)$ is cyclic for all $P \in \mathcal{P}$.

(b) $L(P) = L'(P)$ is cyclic for all $P = [i, 0, \dots, 0]$, $0 \leq i \leq \ell$.

Proof. This follows from Theorem 6.1, since in a uniserial module every term of the socle series is generated by any element not belonging to the previous term.

6.3 Theorem Let

$$A = x_m(\ell^m + \dots + \ell + 1) + x_{m-1}(\ell^{m-1} + \dots + \ell + 1) + \dots + x_1(\ell + 1) + x_0 + 1,$$

$$Z = x_m(d\ell^m + \dots + \ell + 1) + x_{m-1}(d\ell^{m-1} + \dots + \ell + 1) + \dots + x_1(d\ell + 1) + x_0d + 1,$$

$$C = x_m(\ell^{m-1} + \dots + \ell + 1) + x_{m-1}(\ell^{m-2} + \dots + \ell + 1) + \dots + x_2(\ell + 1) + x_1 + 1,$$

noting that $C = 1$ if $m = 0$. Then

(a) $V = C + X$, where X is the amount of values $\phi(Q)$ satisfying $0 \leq \phi(Q) < d\lfloor n/e \rfloor$.

Moreover, $X \geq \lfloor n/e \rfloor$, so $A \leq V \leq Z$.

(b) Suppose $\lfloor n/e \rfloor \geq d\ell$. Then $V = Z - d^2\ell + Y$, where Y is the total amount of values $\phi(Q)$ satisfying $0 \leq \phi(Q) < d^2\ell$. Moreover, $Y \geq \ell d(d+1)/2$, so $Z - \ell d(d-1)/2 \leq V \leq Z$. In fact, if $d \leq \ell$ then $Y = \ell d(d+1)/2$, so $V = Z - \ell d(d-1)/2$, that is

$$V = x_m(d\ell^m + \dots + \ell + 1) + x_{m-1}(d\ell^{m-1} + \dots + \ell + 1) + \dots + x_1(d\ell + 1) + x_0d + 1 - \ell d(d-1)/2.$$

Proof. We may replace \mathcal{P} by \mathcal{P}^* in the statement of the theorem in view of Theorem 4.3.

We will create a sequence of parabolic subgroups in \mathcal{P}^* starting at $G^* = [x_0, x_1, \dots, x_m]$ and ending at $[\lfloor n/e \rfloor, 0, \dots, 0]$. Our sequence will satisfy the following properties: if P is a term of the sequence and P' is the next term then $P' \subset P$ and $\phi(P') = \phi(P) - 1$. The number of terms of the sequence will be C . We will use Theorem 4.3 throughout.

The construction is as follows. Let $P \in \mathcal{P}^*$ and suppose P is not of the form $[a, 0, \dots, 0]$. Then $P = [y_0, \dots, y_i, y_{i+1}, 0, \dots, 0]$, where $0 \leq i < m$ and $y_{i+1} \neq 0$. We then define $P' = [y_0, \dots, y_i + \ell, y_{i+1} - 1, 0, \dots, 0]$. Starting at G^* and repeating this process x_m times we reach $[x_0, x_1, \dots, x_{m-1} + x_m\ell, 0]$. Repeating now the process $x_{m-1} + x_m\ell$ times we

reach $[x_0, x_1, \dots, x_{m-2} + x_{m-1}\ell + x_m\ell^2, 0, 0]$, and so on. All in all, our process produces C consecutive values, from $Z - 1 = \phi(G)$ to $d\lfloor n/e \rfloor = \phi(\lfloor n/e \rfloor, 0, \dots, 0]$. This explains (a).

Suppose now $\lfloor n/e \rfloor \geq d\ell$. Given $P = [a, 0, \dots, 0]$, where $d\ell < a \leq \lfloor n/e \rfloor$, define $P^0 = [a - 1, 0, \dots, 0]$. Through a second process we can attain all d numbers from da , excluded, down to $d(a - 1)$, included, as values $\phi(Q)$. Given such $P = [a, 0, \dots, 0]$ define $P^1 = [a - (d\ell + 1), d, 0, \dots, 0]$. Then $\phi(P^1) = \phi(P)$, and we can now apply the first process d times to P^1 until P^0 is reached. Combining this with the above process, all numbers from $\phi(G)$ down to $\phi(\lfloor n/e \rfloor, 0, \dots, 0]$ are attained as values $\phi(Q)$. This creates

$$C + d(\lfloor n/e \rfloor - d\ell) = Z - d^2\ell$$

consecutive values $\phi(Q)$. This explains the first sentence of (b). We next show that $Y \geq \ell d(d+1)/2$. Indeed, if $0 \leq j \leq d-1$ and $j\ell \leq a < d\ell$ then $0 \leq ad + j < d^2\ell$ is attained at $Q = [a - j\ell, j, 0, \dots, 0] \in \mathcal{P}^*$. Thus $Y \geq \ell d + \ell(d-1) + \dots + \ell = \ell d(d+1)/2$, confirming the second sentence of (b). Next we show $Y = d(d+1)/2$ provided $d \leq \ell$. We wish to know when a number $0 \leq h < d^2\ell$ is of the form $\phi(Q)$. Now $d\ell^2 + \ell + 1 \geq d^2\ell + \ell + 1 > d^2\ell$, so any such Q will have to have the form $Q = [x, y, 0, \dots, 0]$. Dividing h by d , we may write $h = ad + j$, where $0 \leq a < d\ell$ and $0 \leq j \leq d-1$. We look for x, y such that $ad + j = \phi(Q) = dx + y(d\ell + 1)$. Congruence modulo d reveals that $y \equiv j \pmod{d}$. But if $y \geq d$ then $y(d\ell + 1) > d^2\ell$. Thus $y = j$. This implies $a = x + j\ell$, so $a \geq j\ell$. The only attained values are the ones described above, which completes the proof of (b).

6.4 Note If $d \leq \ell$ and $\lfloor n/e \rfloor \leq d\ell$ the value of $V = c(L)$ is given in Theorem 8.5. This completes the determination of V in all cases where $d \leq \ell$. Observe that if $\lfloor n/e \rfloor = d\ell$ and $d \leq \ell$ then Theorems 8.5 and 6.3 compute V in different ways, but the answers agree. Indeed, if $d = \ell$ both give $V = \ell^3/2 + \ell^2/2 + \ell + 2$, while if $d < \ell$ the common value is $\ell d(d+1)/2 + d + 1$.

The proof of Theorem 6.3 shows that at least $C - 1$ consecutive top factors of (3) are not zero. When $\lfloor n/e \rfloor \geq d\ell$ at least $Z - 1 - d^2\ell$ of them are non-zero. If $d = 1$ then $A = v = Z = b + 1$ and all factors $L(c)/L(c+1)$, $0 \leq c \leq b$, are non-zero.

6.5 Theorem (a) If $d = 1$ then (3) is the socle series of L . (The 0 module and all prior repeated terms of (3) must be removed when interpreting this statement)

(b) Let $P \in \mathcal{P}$. Then $\text{soc}(L/L(P)^\#) = L(P)/L(P)^\#$, except for the possibility that $(L'(Q) + L(P)^\#)/L(P)^\#$ be also irreducible, where $Q = [a, 0, \dots, 0]$, $\ell \leq a - 1 < \lfloor n/e \rfloor$ and $d(a - 1) < \phi(P) < da$. In particular, $\text{soc}(L/L(P)^\#) = L(P)/L(P)^\#$ if $\phi(P) \geq d\lfloor n/e \rfloor$.

Proof. Since $L/L(P)^\#$ is completely reducible, we always have $L(P)/L(P)^\# \subseteq \text{soc}(L/L(P)^\#)$. We also know that $L(B) = \text{soc}(L)$, so equality holds for $P = B$.

Suppose $\phi(P) > 0$. By Proposition 2.4 an arbitrary irreducible submodule of $L/L(P)^\#$ must have the form $M = (L'(Q) + L(P)^\#)/L(P)^\#$, where $Q \in \mathcal{P}^*$ and $\phi(Q) \geq \phi(P)$. Choose Q so that $\phi(Q)$ is as small as possible. If $\phi(Q) = \phi(P)$ then $M \subseteq L(P)/L(P)^\#$.

Suppose, if possible, that $\phi(Q) > \phi(P)$. If $d = 1$ the proof of Theorem 6.3 shows that Q contains a parabolic subgroup Q' such that $\phi(Q') = \phi(Q) - 1 \geq \phi(P)$. By Theorem 4.1 we have $L'(Q') \subseteq L(Q)$, so the minimality of Q is violated. Therefore, if $d = 1$ we must have $\phi(Q) = \phi(P)$, whence $M \subseteq L(P)/L(P)^\#$ and a fortiori $L(P)/L(P)^\# = \text{soc}(L/L(P)^\#)$. Induction then gives (a). If d is now arbitrary the proof of Theorem 6.3 yields the same contradiction as long as Q is not of the form $[a, 0, \dots, 0]$. Thus the case $\phi(Q) > \phi(P)$ can only occur when $Q = [a, 0, \dots, 0]$. Since $Q \in \mathcal{P}$ we must have $a \leq \lfloor n/e \rfloor$. As $\phi(P) < \phi(Q)$ we also have $0 < a$ and $\phi(P) < da \leq d\lfloor n/e \rfloor$. Now $[a - 1, \dots, 0] \subset Q$, so using Theorem 4.1 once more yields $\phi(P) > (a - 1)d$. Since below $d\ell$ all values taken by ϕ decrease by d , it is also clear that $a - 1$ must be at least ℓ . This proves (b).

6.6 Proposition (cf. Lemma 5.1) Suppose $d = 1$. Then for every \mathcal{P} -value c , the KG -module $L(c)$ is the sum of all $L'(P)$ with $P \in \mathcal{P}^*(c)$.

Proof. The result is true for the irreducible module $L(b) = L'(B)$. Suppose c is a \mathcal{P} -value smaller than b and the result is true for the first \mathcal{P} -value a larger than c .

We know from Theorem 4.6 that $L(c)$ equals $L(a)$ plus the sum of submodules $L'(P)$ such that $P \in \mathcal{P}^*(c)$. By inductive hypothesis, $L(a)$ is the sum of all $L'(Q)$ such that $Q \in \mathcal{P}^*(a)$. Let $Q \in \mathcal{P}^*(a)$. By Theorem 4.1, it suffices to find P such that $P \in \mathcal{P}^*(c)$ and Q is equivalent to a parabolic subgroup contained in P . Let us write $Q = [y_0, \dots, y_m]$.

If for any $i < m$ we have $y_i > \ell$ we can let P be obtained from Q by replacing y_i by $y_i - \ell$ and y_{i+1} by $y_{i+1} + 1$. We may therefore assume in what follows that $y_i < \ell$ for all $i < m$. Let $y_{-1} = n - e(y_0 + y_1\ell + \cdots + y_m\ell^m)$ and $x_{-1} = n - e\lfloor n/e \rfloor$. We wish to show that $y_{-1} \geq e$, in which case $P = [y_0 + 1, y_1, \dots, y_m] \in \mathcal{P}$. Using the hypothesis $d = 1$ at this single point in the entire proof ensures that P satisfies our requirements.

We proceed to show that $y_{-1} \geq e$. Recalling that $\lfloor n/e \rfloor = (x_m \dots x_0)_\ell$, we first note that $y_m \leq x_m$. Indeed, if $y_m > x_m$ then $\ell^m y_m \geq \ell^m x_m + \ell^m$. Using that all $x_j \leq \ell - 1$ we easily see that $\ell^m > x_0 + \cdots + x_{m-1}\ell^{m-1}$. Combining these inequalities yields $\ell^m y_m > x_0 + \cdots + x_{m-1}\ell^{m-1} + x_m\ell^m = \lfloor n/e \rfloor$, so $\ell^m y_m \geq \lfloor n/e \rfloor + 1$, whence $e\ell^m y_m \geq e(\lfloor n/e \rfloor + 1) > n$, contradicting the fact that $Q \in \mathcal{P}$.

Since $a > c \geq 0$, Theorem 4.3 eliminates the possibility that $(y_m, \dots, y_0) = (x_m, \dots, x_0)$. Scan these sequences from left to right and let i be the first index satisfying $x_i \neq y_i$. Now argue as above, using $y_m = x_m, \dots, y_{i+1} = x_{i+1}$, to see that $y_i > x_i$ is impossible, so $y_i < x_i$. Suppose by way of contradiction that $y_{-1} < e$. Now

$$0 = (x_{-1} + e(x_0 + \cdots + x_{i-1}\ell^{i-1} + x_i\ell^i)) - (y_{-1} + e(y_0 + \cdots + y_{i-1}\ell^{i-1} + y_i\ell^i)).$$

The largest possible value for the second summand is

$$(e - 1) + e(\ell - 1 + \cdots + (\ell - 1)\ell^{i-1} + (x_i - 1)\ell^i),$$

namely

$$(e - 1) + e(\ell - 1)(1 + \cdots + \ell^{i-1}) + e(x_i - 1)\ell^i = (e - 1) + e(\ell^i - 1) + e(x_i - 1)\ell^i = ex_i\ell^i - 1,$$

while the smallest possible value for the first summand is $ex_i\ell$. This absurdity shows that $y_{-1} \geq e$, thereby completing the proof.

6.7 Theorem If $d = 1$ then (3) (all repetitions removed) is the radical series of L .

Proof. By convention $rad^0(L) = L$. Suppose $L(P)$ is a term of the radical series of L . We wish to show that $rad(L(P))$ is $L(P)^\sharp$ (this will give a slightly different proof of Theorem 4.11). Since $L(P)/L(P)^\sharp$ is completely reducible, it follows that $L(P)^\sharp$ contains

$rad(L(P))$. Suppose by way of contradiction that the inclusion is proper. Then the non-zero KG -module $M = L(P)^\sharp / rad(L(P))$ must have a linear character λ of U . By (11) any such λ must satisfy $\vartheta(P(\lambda)) > \vartheta(P)$. Now $L(P)/rad(L(P))$ is completely reducible, so its submodule M is also a factor. Thus M is a factor of $L(P)$. By Proposition 6.6, any non-zero image of $L(P)$ must necessarily contain a linear character μ of U such that $\vartheta(P(\mu)) = \vartheta(P)$. As remarked above, M does not contain any such μ , a contradiction.

7 Comparing various Steinberg lattices

7.1 Theorem (a) $I(c)/I(c+1) \cong (L/L(c+1))^*$ ($*$ = dual) as KG -modules, $c \geq 0$.

(b) For any $c \geq 0$ the composition factors of the KG -module $I(c)/I(c+1)$ are the composition factors of $L(0)/L(1), \dots, L(c)/L(c+1)$ taken together.

(c) $I(0)/I(1) \cong L(0)/L(1)$.

(d) $I(c)/I(c+1) \cong L^*$ as KG -modules for all $c \geq b$.

Proof. (a) Identify K with $\ell^c R / \ell^{c+1} R$ and consider the RG -homomorphism from $I(c)$ to $(L/L(c+1))^*$ given by $x \mapsto \varphi_x$, where $\varphi_x((y + \ell I) + L(c+1)) = f(x, y) + \ell^{c+1} R$ for all $x \in I(c)$, $y \in I$, and f is the bilinear form previously defined on I . Using results from Section 4 of [4] we see that our map has kernel $I(c+1)$ and that $I(c)/I(c+1)$ and $L/L(c+1)$ have the same dimension, as required.

(b) The composition factors of $(L/L(c+1))^*$ are dual to those of $L/L(c+1)$ (in reversed order). The composition factors of $L/L(c+1)$ are those of $L(0)/L(1), \dots, L(c)/L(c+1)$, taken together, and these are all self-dual, so the result follows from (a).

Alternatively, for $0 \leq i \leq c$ there is a natural RG -epimorphism from $I(c+1) + \ell^i I(c-i)$ to $L(c-i)/L(c-i+1)$, with kernel $I(c+1) + \ell^{i+1} I(c-(i+1))$ if $i \leq c-1$ and $I(c+1)$ if $i = c$.

(c) As $L/L(1)$ is self-dual, this follows from (a). Alternatively, the natural epimorphism $I \rightarrow L/L(1)$ has kernel $\ell I + I(1) = I(1)$.

(d) Since $L(c+1) = 0$ for all $c \geq b$, this follows from (a).

7.2 Theorem Let $0 \leq c < h$. Suppose there is a \mathcal{P} -value a such that $c < a \leq h$. (In particular, this applies when h is a \mathcal{P} -value and when $c < h$ are both \mathcal{P} -values.) Consider the Steinberg lattices $I(c)$ and $I(h)$ and let $T^c = I(c)/\ell I(c)$ and $T^h = I(h)/\ell I(h)$ be their respective reductions modulo ℓ . Then the KG -modules T^c and T^h are not isomorphic. Consequently, the RG -modules $I(c)$ and $I(h)$ are not isomorphic.

On the other hand, $I(b) \cong I(b+1) \cong I(b+2) \cong \dots$, so $T^b \cong T^{b+1} \cong T^{b+2} \cong \dots$.

Proof. The maps $v \mapsto \ell v \mapsto \ell^2 v \mapsto \dots$ yield isomorphisms $I(b) \cong I(b+1) \cong I(b+2) \cong \dots$, thereby justifying the last assertion. Thanks to it, we may assume that $h \leq b$. We choose the \mathcal{P} -value a to be as large as possible subject to $a \leq h$.

We have

$$I(c+1)/\ell I(c) = I(c+1)/I(c+1) \cap \ell I \cong (I(c+1) + \ell I)/\ell I = L(c+1),$$

while by Theorem 7.1

$$(I(c)/\ell I(c))/(I(c+1)/\ell I(c)) \cong I(c)/I(c+1) \cong (L/L(c+1))^*.$$

Thus T^c has a submodule isomorphic to $L(c+1)$ and the corresponding factor is isomorphic to $(L/L(c+1))^*$. The analogous result is valid for T^h . Suppose there is an isomorphism from T^c into T^h . Now $L(c+1)$, and hence T^c , has a submodule isomorphic to $L(b)$. Likewise, T^h has a submodule isomorphic to $L(b)$, unless $h = b$, in which case we must omit this part of the proof and proceed to the next paragraph. Now the ℓ -modular reduction of any Steinberg lattice is multiplicity free. Indeed, this just depends on the following facts: U acts on it via the regular representation; $\ell \nmid |U|$; any non-zero KG -module must have a common eigenvector for U . Since $M(b) = L(b)$ is completely reducible, it follows that the supposed isomorphism must map the one copy of $L(b)$ inside T^c into the one copy of $L(b)$ inside T^h . This induces an isomorphism between the corresponding quotients. This process can be continued.

Eventually, we get an isomorphism between a module X with a submodule isomorphic to $L(c+1)/L(h+1)$ with factor isomorphic to $(L/L(c+1))^*$, and a module Y isomorphic to $(L/L(h+1))^*$. If h is a \mathcal{P} -value then $a = h$, whereas if h is not a \mathcal{P} -value then $L(a+1) = \dots = L(h+1)$. In any case, we may replace h by a in the previous sentence.

Now X has a submodule isomorphic to $M(a)$. But Y does not have such a submodule. For if it did, the dual of Y , namely $L/L(a+1)$, would have a factor isomorphic to the self-dual module $M(a)$. Then L would have the completely reducible module $M(a)$ as image. But $M(a) \neq 0$, since a is a \mathcal{P} -value, and L has only one non-zero completely reducible image, up to isomorphism, namely the irreducible module $M(0) = L/L(1)$, as the radical $L(1)$ of L is maximal. It would follow that $M(0) \cong M(a)$, which is impossible since $a > 0$ and L is multiplicity free.

7.3 Note As mentioned above, for any $c \geq 0$, the KG -module T^c has a submodule isomorphic to $L(c+1)$ with a factor isomorphic to $(L/L(c+1))^*$. Combining this with Theorem 7.1, we see directly that all T^c , $c \geq 0$, have the same composition factors, as predicted by the Brauer-Nesbitt theorem.

7.4 Proposition If $0 < c < b$ then $\text{soc}(T^c)$ contains copies of the non-isomorphic irreducible modules $M(b) = L(b)$ and $M(0)$. In particular, $\text{soc}(T^c)$ is not irreducible.

Proof. The proof of Theorem 7.2 shows that $L(b)$ is inside T^c for all $0 \leq c < b$. The map $v \mapsto \ell^c v$ from I into $I(c)$ sends ℓI into $\ell I(c)$, inducing a map from L into T^c . Suppose $c > 0$. Let $\lambda : U \rightarrow R^*$ be a group homomorphism such that $P(\lambda) = G$. Then $\ell^c E_\lambda$ is in $I(c)$ but not in $I(c+1)$, which shows that the map $L \rightarrow T^c$ is not zero. However, using $c > 0$ we easily see that $L(1)$ is in the kernel. Since $L(1)$ is maximal, it follows that $M(0) = L/L(1)$ embeds into T^c , as claimed.

7.5 Note $T^b \cong L^*$, since $T^b = I(b)/\ell I(b) = I(b)/I(b+1) \cong (L/L(b+1))^* = L^*$.

8 Positive cases of Gow's conjecture

- 8.1 Theorem** (a) If $d \leq \ell$ then (3) is a composition series of L provided $\lfloor n/e \rfloor \leq d\ell$.
(b) If $d = \ell + 1$ then (3) is a composition series of L provided $\lfloor n/e \rfloor \leq \ell^2$.
(c) If $d > \ell + 1$ then (3) is a composition series of L provided $\lfloor n/e \rfloor < \ell^2 + \ell$.

Proof. This follows from Corollary 4.7 via Lemma 12.4 of Appendix C.

8.2 Note If $d = 1$ Theorem 8.1 does not add much to Ackermann's contribution, as we would just be passing from $\lfloor n/e \rfloor < \ell$ to $\lfloor n/e \rfloor \leq \ell$. How large can d be? If $\ell \mid q - 1$ and ℓ is odd then necessarily $d = 1$. However, if ℓ is odd, $2 \leq e$ and $e \mid \ell - 1$, or if $\ell = 2 = e$, then there are infinitely many primes q such that $q \neq \ell$,

$$e = e(\ell, q) = \min\{i \geq 2 \mid \ell \text{ divides } \frac{q^i - 1}{q - 1}\}$$

and $d > \ell + 1$. This follows easily from Dirichlet's Theorem on primes in arithmetic progression (see Lemma 8.3 below for details). If q is any of these primes then (13) is a composition series of L as long as $\lfloor n/e \rfloor < \ell^2 + \ell$.

8.3 Lemma Let ℓ be a prime. If $\ell \mid q - 1$ and ℓ is odd then $d = 1$. Suppose that either $\ell = 2 = e$, or ℓ is odd, $2 \leq e$ and $e \mid \ell - 1$. Let $s \geq 1$. Then there are infinitely many primes q such that $q \neq \ell$, $e = e(\ell, q)$ and $d = \nu_\ell(\frac{q^e - 1}{q - 1}) \geq s$.

Proof. The first assertion follows from the proof of Lemma 11.1 (just replace es by 1).

Suppose still that ℓ is odd. Associated to any $m \geq 1$ we have the multiplicative group $U(m) = \{[a] \mid \gcd(a, m) = 1\}$. Clearly $U(\ell^s)$ decomposes as the direct product of the kernel, say A , of $U(\ell^s) \rightarrow U(\ell)$, and a unique subgroup B isomorphic to $U(\ell)$. It follows that $U(\ell^s) \rightarrow U(\ell)$ preserves the order of any element whose order divides $\ell - 1$, where all these orders occur since $U(\ell^s)$ is cyclic of order $(\ell - 1)\ell^{s-1}$.

Given e as stated, let t be an integer relatively prime to ℓ having order e modulo ℓ^s . By Dirichlet's Theorem there are infinitely many primes congruent to t modulo ℓ^s . Let q be one of them. Clearly $q \neq \ell$. The remarks made above ensure that the order of q modulo ℓ is e . As $e > 1$, we infer $e = e(\ell, q)$. Moreover, $q^e \equiv t^e \equiv 1 \pmod{\ell^s}$, so $d \geq s$.

Suppose next $\ell = 2$. By Dirichlet's Theorem there are infinitely many primes congruent to -1 modulo 2^s , as required.

8.4 Lemma For $i \geq -1$ let $\Lambda_i(n)$ be the total number of parabolic subgroups of the form $[z_{-1}, z_0, \dots, z_i, 0, \dots, 0]$ in \mathcal{P}^* , as defined in (14). Then $\Lambda_{-1}(n) = 1$,

$$\Lambda_i(n) = \sum_{0 \leq j \leq \lfloor n/e\ell^i \rfloor} \Lambda_{i-1}(n - e\ell^i j), \quad 0 \leq i \leq m,$$

and $|\mathcal{P}^*| = \Delta_m(n)$.

Proof. This is clear.

8.5 Theorem Suppose the conditions of Theorem 8.1 are satisfied, that is, assume $\lfloor n/e \rfloor \leq d\ell$ if $d \leq \ell$; $\lfloor n/e \rfloor \leq \ell^2$ if $d = \ell + 1$; $\lfloor n/e \rfloor < \ell^2 + \ell$ if $d > \ell + 1$. Then

- (a) $c(L) = V = |\mathcal{P}^*| = \lfloor n/e \rfloor + 1$ if $m = 0$.
- (b) $c(L) = V = |\mathcal{P}^*| = (x_1 + 1)(\frac{x_1}{2}\ell + x_0 + 1)$ if $m = 1$ and $\lfloor n/e \rfloor = (x_1 x_0)_\ell$.
- (c) $c(L) = V = |\mathcal{P}^*| = \frac{1}{2}\ell^3 + \frac{1}{2}\ell^2 + (x_0 + 1)\ell + 2(x_0 + 1)$ if $m = 2$ and $\lfloor n/e \rfloor = (1, 0, x_0)_\ell$.

Proof. We have $c(L) = V$ by Theorem 8.1 and $V = |\mathcal{P}^*|$ by Theorem 4.3 and Lemma 12.4 of Appendix C. The exact value of $|\mathcal{P}^*|$ can be computed by means of Lemma 8.4.

9 Examples

9.1 Example Suppose $n = 6$, $\ell = 2$, $q = 5$. In this case, all numbers from 0 to $4 = \vartheta(B)$ are \mathcal{P} -values. Thus $V = 5$, whereas $|\mathcal{P}^*| = 6$. The 3 bottom factors $M(4)$, $M(3)$, $M(2)$ as well as the top factor $M(0)$ are irreducible. Consider the parabolic subgroups $P = (2, 2, 2)$ and $Q = (4, 1, 1)$, where the numbers indicate the sizes of the diagonal blocks. Then $P, Q \in \mathcal{P}^*(1)$, and James table for $n = 6$ adjusted to the prime $\ell = 2$ implies that $M(1) = N(P) \oplus N(Q)$ is not irreducible.

9.2 Example Suppose $\ell = 2$, $e = 2$, $n = 10$ and $d = 1$ (say $q = 5$). Then $V = 9$, whereas $|\mathcal{P}^*| = 14$. The 14 members of \mathcal{P}^* are distributed into \mathcal{P} -values as follows, using an obvious notation for partitions:

$$(82) \in \mathcal{P}^*(0); (442), (81^2) \in \mathcal{P}^*(1); (4^2 1^2), (42^3) \in \mathcal{P}^*(2); (2^5), (42^2 1^2) \in \mathcal{P}^*(3);$$

$$(2^4 1^2), (421^4) \in \mathcal{P}^*(4); (2^3 1^4), (41^6) \in \mathcal{P}^*(5); (2^2 1^6) \in \mathcal{P}^*(6); (21^8) \in \mathcal{P}^*(7); (1^{10}) \in \mathcal{P}^*(8).$$

As predicted, the 3 bottom factors $M(8)$, $M(7)$, $M(6)$ as well as the top factor $M(0)$ are irreducible. Refer now to [3] and use the decomposition matrix from page 257 together with the adjustment matrix from page 258. We see that $c(L) = 14$. It follows that all 5 doubtful factors of L , namely $M(1)$ through $M(5)$, fail to be irreducible, and are equal

to the direct sum of the two irreducible constituents $N(P), N(Q)$, where P and Q are as displayed above for each \mathcal{P} -value $1 \leq c \leq 5$.

10 Appendix A

The goal of this section is to furnish a proof of Theorem 4.1.

10.1 Calculations in the Steinberg lattice

Let $\sigma \in S_n$. The set $I(\sigma)$, of inversions of σ , is formed by all pairs (i, j) such that $1 \leq i < j \leq n$ but $\sigma(i) > \sigma(j)$. We associate to σ the subgroup U_σ^+ formed by all $u \in U$ such that $\sigma u \sigma^{-1} \in U$, and also the subgroup U_σ^- formed by all $u \in U$ such that $\sigma u \sigma^{-1} \in V$, the lower unitriangular group. We fix a well-order on $\Phi = \{(i, j) \mid 1 \leq i < j \leq n\}$. Following this order, we can write any $u \in U_\sigma^+$ and $v \in U_\sigma^-$ in the form

$$u = \prod_{r \notin I(\sigma)} t_r(a_r) \text{ and } v = \prod_{s \in I(\sigma)} t_s(b_s), \quad (15)$$

for unique $a_r, b_s \in F_q$. We have

$$U_\sigma^+ U_\sigma^- = U = U_\sigma^- U_\sigma^+ \quad \text{and} \quad U_\sigma^+ \cap U_\sigma^- = 1. \quad (16)$$

For the special permutation

$$\sigma_0 = (1, n)(2, n-1)(3, n-2) \cdots = \sigma_0^{-1} \quad (17)$$

we have $I(\sigma_0) = \Phi$, so that

$$U_{\sigma_0}^- = U \quad \text{and} \quad U_{\sigma_0}^+ = 1. \quad (18)$$

Moreover,

$$I(\sigma_0 \sigma) = \Phi \setminus I(\sigma) \quad \text{and} \quad U_{\sigma_0 \sigma}^+ = U_\sigma^-. \quad (19)$$

The subset $\{g\hat{B} \mid g \in G\}$ of RG is linearly independent, so it is an R -basis for its span, say Y . Note that I is contained in Y . If $x \in I$ it is then clear what we mean by “the coefficient of $g\hat{B}$ in x ”, a phrase that will be used at critical points below. Of course, we

may have $g\widehat{B} = h\widehat{B}$ for $g, h \in G$, which happens if and only if $gB = hB$. We can avoid repetitions by means of the Bruhat decomposition. Thus, a basis for Y is formed by all $u\sigma\widehat{B}$, where $\sigma \in S_n$ and $u \in U_{\sigma^{-1}}^-$.

The following two results are valid in the more general context used in [4].

10.1 Lemma Let $\lambda : U \rightarrow R^*$ be a group homomorphism with E_λ as in (6). Then

$$E_\lambda = \sum_{\sigma \in S_n} \sum_{u \in U_{\sigma^{-1}}^-} sg(\sigma) C_\sigma(\lambda) \lambda(u) u \sigma \widehat{B}, \quad (20)$$

where

$$C_\sigma(\lambda) = \sum_{v \in U_{\sigma^{-1}}^+} \lambda(v) = \begin{cases} |U_{\sigma^{-1}}^+| & \text{if } \lambda \text{ is trivial on } U_{\sigma^{-1}}^+, \\ 0 & \text{otherwise.} \end{cases} \quad (21)$$

Proof. According to the definitions (1) of ε and (6) of E_λ we have

$$E_\lambda = \sum_{u \in U} \lambda(u) u \sum_{\sigma \in S_n} sg(\sigma) \sigma \widehat{B} = \sum_{\sigma \in S_n} \sum_{u \in U} sg(\sigma) \lambda(u) u \sigma \widehat{B}.$$

We now use the decomposition (16) of U , the fact that $\sigma^{-1}v\sigma\widehat{B} = \widehat{B}$ for all $v \in U_{\sigma^{-1}}^+$, and that λ is a group homomorphism to obtain (20). The displayed value of $C_\sigma(\lambda)$ is clear.

10.2 Lemma Let $\sigma \in S_n$. Let $\lambda, \mu : U \rightarrow R^*$ be group homomorphisms. Suppose that every X_r , $r \in \Pi$, acts on the element $\widehat{U_{\sigma^{-1}}^-} \cdot \sigma \cdot E_\lambda$ of I via μ^{-1} . Then

$$\widehat{U_{\sigma^{-1}}^-} \cdot \sigma \cdot E_\lambda = sg(\sigma) E_\mu.$$

Proof. Since the X_r , $r \in \Pi$, generate U , it follows that U acts on $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$ via μ^{-1} . But U acts on I via the regular representation. We deduce that $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$ must be a scalar multiple of E_μ , that is

$$\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda = a E_\mu, \quad (22)$$

where $a \in R$ is to be found. To determine a we write both sides of (22) relative to the basis $\{g\widehat{B} \mid g \in G\}$ of Y previously mentioned, and compare coefficients. In view of (22), it suffices to compare coefficients in a *single* basis vector $g\widehat{B}$, provided the coefficient of $g\widehat{B}$ in E_μ is not zero. A good choice turns out to be $\sigma\sigma_0\widehat{B}$, where σ_0 is defined in (17).

By (20) and (18), the coefficient of $\sigma_0 \hat{B}$ in E_λ is equal to $sg(\sigma_0)$. Multiplication by σ simply shifts all basis vectors, so the coefficient of $\sigma\sigma_0 \hat{B}$ in σE_λ is also $sg(\sigma_0)$.

Now by (19)

$$U_{(\sigma\sigma_0)^{-1}}^+ = U_{\sigma_0^{-1}\sigma^{-1}}^+ = U_{\sigma_0\sigma^{-1}}^+ = U_{\sigma^{-1}}^-.$$

Thus if $u \in U_{\sigma^{-1}}^- = U_{(\sigma\sigma_0)^{-1}}^+$ then

$$u\sigma\sigma_0 \hat{B} = \sigma\sigma_0[(\sigma\sigma_0)^{-1}u\sigma\sigma_0]\hat{B} = \sigma\sigma_0 \hat{B},$$

so multiplying σE_λ by u fixes the basis vector $\sigma\sigma_0 \hat{B}$. This happens for the $|U_{\sigma^{-1}}^-|$ vectors u in $U_{\sigma^{-1}}^-$, which, so far, will produce the coefficient $sg(\sigma_0)|U_{\sigma^{-1}}^-|$ for $\sigma\sigma_0 \hat{B}$ in $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$.

We must now make sure that the basis vector $\sigma\sigma_0 \hat{B}$ cannot be produced in any other way in $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$. Well, by (20), a typical summand of E_λ has the form $v\tau \hat{B}$, where $\tau \in S_n$ and $v \in U_{\tau^{-1}}^-$. Thus, a typical summand of $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$ will have the form $u\sigma v\tau \hat{B}$, where $u \in U_{\sigma^{-1}}^-$. When will this summand equal $\sigma\sigma_0 \hat{B}$? Well, suppose that $u\sigma v\tau \hat{B} = \sigma\sigma_0 \hat{B}$ for some u, v and τ as stated. The right hand side was shown above to equal $u\sigma\sigma_0 \hat{B}$, which gives $u\sigma v\tau \hat{B} = u\sigma\sigma_0 \hat{B}$, and a fortiori the equation $u\sigma v\tau B = u\sigma\sigma_0 B$ in G . This, in turn, yields $v\tau B = \sigma_0 B$. The uniqueness part of the Bruhat decomposition gives $\tau = \sigma_0$ first, and then $v = 1$, since $U_{\sigma_0}^- = U$. Thus, the basis vector $\sigma\sigma_0 \hat{B}$ appears in $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$ only as described above. Hence the coefficient of $\sigma\sigma_0 \hat{B}$ in $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$ is exactly $sg(\sigma_0)|U_{\sigma^{-1}}^-|$. In particular, $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda \neq 0$.

Observe next that μ is trivial on $U_{\sigma^{-1}}^-$. Indeed, let $u \in U_{\sigma^{-1}}^-$. Clearly, $u\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda = \widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$, while by hypothesis $u\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda = \mu(u)^{-1}\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$. Since I is a torsion free R -module and, by above, $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda \neq 0$, we infer $\mu(u) = 1$.

Finally, due to (20), the coefficient of $\sigma\sigma_0 \hat{B}$ in E_μ is equal to $sg(\sigma\sigma_0)C_{\sigma\sigma_0}(\mu)$. By above μ is trivial on $U_{\sigma^{-1}}^- = U_{(\sigma\sigma_0)^{-1}}^+$. Therefore (21) gives $C_{\sigma\sigma_0}(\mu) = |U_{\sigma^{-1}}^-|$. Hence the coefficient of $\sigma\sigma_0 \hat{B}$ in E_μ is equal to $sg(\sigma)sg(\sigma_0)|U_{\sigma^{-1}}^-|$.

Comparing coefficients yields $a = sg(\sigma)$, as claimed.

10.2 Properties of parabolic subgroups reflected on I

Let $P = (a_1, \dots, a_k)$ be a parabolic subgroup. Replacing any $a_i > 1$ by a subsequence (a, b) such that $a + b = a_i$ produces a parabolic subgroup contained in P , and any parabolic

subgroup contained in P can be obtained by repeated application of this procedure.

Let J be the subset of Π corresponding to P . It is clear what we mean by the connected components of J . We next describe how these can be read off from (a_1, \dots, a_k) . If $a_1 = 1$ then $(1, 2)$ is not in J , while if $a_1 > 1$ then all of $(1, 2), \dots, (a_1 - 1, a_1)$ are in J but $(a_1, a_1 + 1)$ is not in J . The same procedure is applied to a_2, \dots, a_k , starting at the first element of Π whose inclusion in J was not decided in the previous steps. For instance, $P = (2, 1, 2)$ produces $J = \{(1, 2), (4, 5)\}$. Each $a_i > 1$ gives rise to a connected component of J of length $a_i - 1$, and every connected component of J arises in this way. Let Q be the parabolic subgroup obtained from J by a single switching $a_i \leftrightarrow a_{i+1}$. Let J' be the subset of Π associated to Q . How is J' obtained from J ? This is obvious, but later applications of Lemma 10.2 will require an explicit answer. Four cases arise:

- Suppose $a_i = a_{i+1} = 1$. Then $J' = J$.
- Suppose $a_i > 1$ and $a_{i+1} > 1$. Let

$$A = \{(j, j+1), \dots, (j+m-1, j+m)\}, \quad m \geq 1$$

and

$$B = \{(j+m+1, j+m+2), \dots, (j+m+s, j+m+s+1)\}, \quad s \geq 1$$

be the connected components of J corresponding to $a_i = m+1$ and $a_{i+1} = s+1$. Then the connected components of J' are precisely those of J , except for A , which must be replaced by

$$A' = \{(j, j+1), \dots, (j+s-1, j+s)\},$$

and for B , which must be replaced by

$$B' = \{(j+s+1, j+s+2), \dots, (j+s+m, j+s+m+1)\}.$$

Of course, $J' = J$ if $a_i = a_{i+1}$. Note that $(j+m, j+m+1) \notin J$, while $(j+s, j+s+1) \notin J'$.

- Suppose $a_i > 1$ and $a_{i+1} = 1$. Then $a_i = m+1$, where $m \geq 1$. Denote by $A = \{(j, j+1), \dots, (j+m-1, j+m)\}$ the connected component of J associated to a_i . In this case J' has the same connected components as J , except for A , which must be replaced by $A' = \{(j+1, j+2), \dots, (j+m, j+m+1)\}$.

• Suppose $a_i = 1$ and $a_{i+1} > 1$. Then $a_{i+1} = s + 1$, where $s \geq 1$. Denote by $A = \{(j+1, j+2), \dots, (j+s, j+s+1)\}$ the connected component of J associated to a_{i+1} . In this case J' has the same connected components as J , except for A , which must be replaced by $A' = \{(j, j+1), \dots, (j+s-1, j+s)\}$.

10.3 Theorem If $P, Q \in \mathcal{P}$ are equivalent then $I'(P) = I'(Q)$.

Proof. Let $P = (a_1, \dots, a_k)$ and let J be the subset of Π associated to P . It suffices to prove the theorem when Q is obtained from P by a single switching $a_i \leftrightarrow a_{i+1}$. Let J' be the subset of Π associated to Q .

Our main tool will be Lemma 10.2. Once the right choice of $\sigma \in S_n$ is made, it is then a matter of routine to verify that the hypotheses of Lemma 10.2 are met.

We refer to the notation introduced earlier in this section for this scenario. Of the four given cases, we only need to consider the last three. Let us begin with the first of these, namely when $a_i > 1$ and $a_{i+1} > 1$.

Let $\sigma \in S_n$ fix every point outside of the interval $[j, \dots, j+m+s+1]$ and be defined as follows on this interval:

$$\begin{array}{ccccccc} j & \cdots & j+m & j+m+1 & \cdots & j+m+s+1 \\ \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow \\ j+s+1 & \cdots & j+m+s+1 & j & \cdots & j+s \end{array}$$

Notice that

$$\sigma A \sigma^{-1} = B' \text{ and } \sigma B \sigma^{-1} = A'.$$

Thus $\sigma J \sigma^{-1} = J'$ and conjugation by σ sends the connected components of J into those of J' .

Clearly conjugation by the non-trivial permutation σ cannot preserve Π . In this case, the following subsets of Π are sent outside of Π : the “middle” set $C = \{(j+m, j+m+1)\}$ and the “boundary” set $D = \{(j-1, j), (j+m+s+1, j+m+s+2)\} \cap \Pi$. Also notice that conjugation by σ does not send P into Q either. Indeed, if $s \neq m$ then $P \neq Q$, and distinct standard parabolic subgroups cannot be conjugate, while if $s = m$ then $P = Q$, but still $\sigma \notin P$, and P is self-normalizing.

Let $\lambda : U \rightarrow R^*$ be a group homomorphism such that $P(\lambda) = P$. We next define a group homomorphism $\mu : U \rightarrow R^*$ such that $P(\mu) = Q$. It suffices to define a group homomorphism on every X_r , $r \in \Pi$, as these will have a unique extension to U (we use here that there are exactly $|U/U'|$ homomorphisms $U \rightarrow R^*$, given that U/U' is an elementary abelian p -group and R has a non-trivial p -root of unity). We simply let

$$\mu(t_r(a)) = \lambda(t_{\sigma^{-1}r\sigma}(a)), \quad r \in J' \quad (23)$$

and

$$\mu(t_r(a)) = 1, \quad r \in \Pi \setminus J'. \quad (24)$$

By construction, $P(\mu) = Q$.

By virtue of Lemma 10.2, all we have to do now is verify that each fundamental root subgroup acts on $\widehat{U_{\sigma^{-1}}^-} \cdot \sigma \cdot E_\lambda$ via μ^{-1} . Indeed, this will show that $I'(Q) \subseteq I'(P)$, and switching back a_i and a_{i+1} will yield the reverse inclusion.

Note first of all that

$$I(\sigma^{-1}) = \{(a, b) \mid j \leq a \leq j + s, \quad j + s + 1 \leq b \leq j + m + s + 1\}. \quad (25)$$

We next verify that each X_r , $r \in \Pi$, acts on $\widehat{U_{\sigma^{-1}}^-} \cdot \sigma \cdot E_\lambda$ via μ^{-1} . Now Π decomposes as $\Pi = A' \cup B' \cup C' \cup D \cup E$, where $C' = \{(j + s, j + s + 1)\}$, A' , B' and D have been defined above, and E is the complement of $A' \cup B' \cup C' \cup D$ in Π . Our argument is divided according to this decomposition.

If r is in E then X_r normalizes $U_{\sigma^{-1}}^-$ and commutes elementwise with σ , so it acts on $U_{\sigma^{-1}}^- \sigma E_\lambda$ via λ^{-1} , and hence via μ^{-1} , as they agree on X_r .

If $r = (j + s, j + s + 1)$ then X_r is included in $U_{\sigma^{-1}}^-$, so it acts trivially on $\widehat{U_{\sigma^{-1}}^-} \sigma E_\lambda$, and hence via μ^{-1} , since, as remarked earlier, $(j + s, j + s + 1) \notin J'$.

Consider next the case when $r \in A' \cup B'$. We will make use of the well-known formula:

$$\sigma t_{ij}(a) \sigma^{-1} = t_{\sigma(i)\sigma(j)}(a), \quad \sigma \in S_n. \quad (26)$$

We will also use the commutator $[xy] = xyx^{-1}y^{-1}$. Clearly if $i < j$, $k < l$ and $i \neq l$ then

$$[t_{ij}(a)t_{kl}(b)] = \begin{cases} t_{il}(ab) & \text{if } j = k, \\ 1 & \text{otherwise.} \end{cases} \quad (27)$$

From (27) and (25) we see that X_r normalizes $U_{\sigma^{-1}}^-$. Thus by (26)

$$t_r(a)\widehat{U_{\sigma^{-1}}^-}\sigma E_\lambda = \widehat{U_{\sigma^{-1}}^-}t_r(a)\sigma E_\lambda = \widehat{U_{\sigma^{-1}}^-}\sigma\sigma^{-1}t_r(a)\sigma E_\lambda = \widehat{U_{\sigma^{-1}}^-}\sigma t_{\sigma^{-1}r\sigma}(a)E_\lambda,$$

where the last term equals

$$\lambda(t_{\sigma^{-1}r\sigma})^{-1}\widehat{U_{\sigma^{-1}}^-}\sigma E_\lambda = \mu(t_r(a))^{-1}\widehat{U_{\sigma^{-1}}^-}\sigma E_\lambda.$$

Suppose finally that r belongs to D . Let us treat the case $r = (j-1, j)$ first. It is no longer true that X_r normalizes $U_{\sigma^{-1}}^-$, so we have to be a bit careful. Let $t_r(\alpha) \in X_r$ and let $u = U_{\sigma^{-1}}^-$. Selecting a suitable ordering, we may use (15) to write $u = u_1 u_2$, where u_1 is a product of factors of the form $t_{ab}(\beta)$, where $(a, b) \in I(\sigma^{-1})$ and $a \neq j$, and u_2 is a product of factors of the form $t_{jb}(\beta)$, where $(j, b) \in I(\sigma^{-1})$. By (27) we have

$$t_r(\alpha)u_1 = u_1 t_r(\alpha).$$

By (27) any $t_{jb}(\beta)$ will commute with any commutator

$$[t_r(\alpha)t_{jc}(\gamma)] = t_{j-1,c}(\delta),$$

where $j+s+1 \leq b, c \leq j+m+s+1$. Repeatedly using this comment and the given expression for u_2 , we see that $t_r(\alpha)u_2 = u_2 t_r(\alpha)z$, where z is a product of factors of form $t_{j-1,c}(\delta)$, where $j+s+1 \leq c \leq j+m+s+1$. Therefore $t_r(\alpha)u = ut_r(\alpha)z$. Now $w = \sigma^{-1}z\sigma$ is a product of factors of the form $t_{j-1,d}(\delta)$, where $j \leq d \leq j+m$. Now if $d > j$ then $t_{j-1,d}(\delta) \in U'$, while $t_{j-1,j}(\delta)$ acts trivially on E_λ , since $(j-1, j) \notin J$. Thus w acts trivially on E_λ . Also $\sigma^{-1}t_{j-1,j}(\alpha)\sigma = t_{j-1,j+m+1}(\alpha) \in U'$ acts trivially on E_λ . All in all, we get that $t_r(\alpha)$ acts trivially on $u\sigma E_\lambda$. As this happens for all $u \in U_{\sigma^{-1}}^-$, we finally obtain that $t_r(\alpha)$ acts trivially on $\widehat{U_{\sigma^{-1}}^-}\sigma E_\lambda$. The reasoning when $r = (j+m+s+1, j+m+s+2)$ is entirely analogous.

This completes the proof of the case $a_i > 1$ and $a_{i+1} > 1$. The case $a_i > 1$ and $a_{i+1} = 1$ can be handled as a degenerate (and simplified) case of the above, corresponding to $s = 0$. Accordingly, we merely need to modify the permutation σ to

$$\begin{array}{cccccc} j & j+1 & \cdots & j+m & j+m+1 \\ \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\ j+1 & j+2 & \cdots & j+m+1 & j \end{array}$$

Similarly, the case $a_i = 1$ and $a_{i+1} > 1$ can also be handled as a degenerate case of the one above, corresponding to $m = 0$. Here we modify σ to the permutation

$$\begin{array}{ccccccccc} j & & j+1 & \cdots & j+s & & j+s+1 & & \\ \downarrow & & \downarrow & \cdots & \downarrow & & \downarrow & & \\ j+s+1 & & j & \cdots & j+s-1 & & j+s & & \end{array}$$

In the notation corresponding to these cases, conjugation by σ will send A to A' and fix all other connected components of J . Given a group homomorphism $\lambda : U \rightarrow R^*$ such that $P = P(\lambda)$, we define μ using the formulae (23) and (24). Again, $P(\mu) = Q$, and one can check that the argument given in the general case will go through in the two degenerate cases above, *mutatis mutandi*.

10.4 Theorem Let $Q \subseteq P$ be parabolic subgroups of G . Then $I'(Q) \subseteq I'(P)$.

Proof. Let J and J' be the subsets of Π associated to P and Q , respectively. We may assume that $J \neq \emptyset$ and $J' \neq J$. By repeatedly removing one point from J at a time, we may assume that J' is obtained by removing a single point, say r , from J . Thus $J' = J \setminus \{r\}$. Let A be the connected component of J to which r belongs. Two cases arise: r is an endpoint or r is a middle point of A .

Now an endpoint can be a left or a right endpoint. A middle point can be skewed to the left, i.e. there are at least as many points in A to the right of it as to the left of it, or skewed to the right. By means of Theorem 10.3 we may reduce ourselves to consider only left endpoints and middle points skewed to the left.

This is so because the bijection $(1, 2) \leftrightarrow (n-1, n), (2, 3) \leftrightarrow (n-2, n-1), \dots$ of Π into itself induces a bijection from \mathcal{P} into itself, which sends a parabolic subgroup into one equivalent to it, and interchanges left and right in both cases above.

By rearranging the blocks of P and using Theorem 10.3, we may also assume that the left endpoint of A is $(1, 2)$. Thus $A = \{(1, 2), \dots, (k-1, k)\}$, where $k > 1$.

Assume first that r is the left endpoint of A , so that $r = (1, 2)$. Then J' has the same connected components as J , except for A , which must now be replaced by $A' = \{(2, 3), \dots, (k-1, k)\}$. Note that $A = \emptyset$ if $k = 2$.

Consider the cycle $\sigma = (1, 2, \dots, k) \in S_n$. Given a group homomorphism $\lambda : U \rightarrow R^*$ such that $P(\lambda) = P$, we define μ using (23) and (24). Then $P(\mu) = Q$. We now apply Lemma 10.2, verifying its hypotheses as in the proof Theorem 10.3.

Suppose next $r = (i, i + 1)$ is a middle point of A skewed to the left. Thus

$$A = \{(1, 2), \dots, (i - 1, i), (i, i + 1), (i + 1, i + 2), \dots, (2i - 1, 2i), \dots, (k - 1, k)\},$$

where $1 < i$ and $2i \leq k$. The connected components of J' are those of J , except that A must be replaced by the two components

$$A' = \{(1, 2), \dots, (i - 1, i)\} \text{ and } B = \{(i + 1, i + 2), \dots, (2i - 1, 2i), \dots, (k - 1, k)\}.$$

Consider the permutation $\sigma \in S_n$ whose inverse σ^{-1} fixes every number larger than k and has the following effect on the interval $[1, \dots, k]$:

$$\begin{array}{cccccccccccc} i+1 & i+2 & \cdots & 2i-1 & 2i & \cdots & k & 1 & 2 & \cdots & i \\ \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ 1 & 2 & \cdots & i-1 & i & \cdots & k-i & k-i+1 & k-i+2 & \cdots & k \end{array}$$

This definition of σ^{-1} yields

$$I(\sigma^{-1}) = \{(a, b) \mid 1 \leq a \leq i, \quad i + 1 \leq b \leq k\}.$$

As usual, a valid application of Lemma 10.2 yields the desired result.

10.5 Note Various special cases suggest that $[P : Q]I'(P) \subseteq I'(Q)$ if $Q \subseteq P$ are in \mathcal{P} .

11 Appendix B

Here we develop auxiliary tools to compute $\nu_\ell([P : B])$. Recall that d is defined in (5) and

$$s_0 = d, s_1 = \ell d + 1, s_2 = \ell^2 d + \ell + 1, s_3 = \ell^3 d + \ell^2 + \ell + 1, \dots$$

For typographical reasons it will be necessary to use the notation

$$\begin{aligned} w(a, b) &= \frac{q^a - 1}{q^b - 1}, \quad w(a) = \frac{q^a - 1}{q - 1}, \quad a, b \geq 1, \\ g(a) &= \nu_\ell(w(a)), \quad h(a) = \nu_\ell(w(1)w(2) \cdots w(a)), \quad a \geq 1. \end{aligned}$$

The following two results are borrowed from [2].

11.1 Lemma Let s be a positive integer. Then

$$\nu_\ell\left[\frac{q^{es\ell} - 1}{q^{es} - 1}\right] = 1.$$

Proof. Suppose first that $\ell = 2$. Then $e = 2$, q is odd and

$$\frac{q^{es2} - 1}{q^{es} - 1} = q^{es} + 1 = (q^s)^2 + 1 \equiv 2 \pmod{4}.$$

Suppose next $\ell > 2$. We have $q^{es} - 1 = a\ell^b$, with a coprime to ℓ and $b \geq 1$. Then

$$\frac{q^{es\ell} - 1}{q^{es} - 1} = \frac{(a\ell^b + 1)^\ell - 1}{a\ell^b} = \sum_{1 \leq i \leq \ell} \binom{\ell}{i} (a\ell^b)^{i-1} \equiv \ell \pmod{\ell^2}.$$

11.2 Lemma Let t be a positive integer. Then

$$\nu_\ell\left[\frac{q^{et} - 1}{q^e - 1}\right] = \nu_\ell(t).$$

Proof. We have $t = c\ell^u$, with c coprime to ℓ . Then

$$\frac{q^{et} - 1}{q^e - 1} = \frac{q^{ec} - 1}{q^e - 1} \times \prod_{1 \leq i \leq u} w(e\ell^i, e\ell^{i-1}).$$

But

$$\frac{q^{ec} - 1}{q^e - 1} \equiv 1 + q^e + \cdots + q^{e(c-1)} \equiv c \not\equiv 0 \pmod{\ell},$$

while ℓ divides each factor $w(e\ell^i, e\ell^{i-1})$ exactly once by Lemma 11.1, so the result follows.

11.3 Lemma $h(e\ell^i) = s_i$ for all $i \geq 0$.

Proof. First note that by Lemma 11.2

$$\nu_\ell(s) = \nu_\ell(t) \Rightarrow g(es) = g(et), \quad s, t \geq 1. \quad (28)$$

Next observe that $\ell \mid w(a)$ if and only if $e \mid a$. It follows from this observation that if $a = be + c$, where $0 \leq b$ and $0 \leq c < e$, then

$$h(a) = \sum_{1 \leq i \leq b} g(ie) = h(be). \quad (29)$$

We deduce from (29) that $h(e) = g(e) = d$, so our formula works if $i = 0$. Suppose $h(e\ell^i) = s_i$ for some $i \geq 0$. Then by (29)

$$h(e\ell^{i+1}) = h(e\ell^i) + \sum_{1 \leq k \leq \ell^i} g(e(k + \ell^i)) + \cdots + \sum_{1 \leq k \leq \ell^i} g(e(k + (\ell - 1)\ell^i)).$$

If $1 \leq k \leq \ell^i$ and $0 \leq j < \ell - 1$, or if $1 \leq k < \ell^i$ and $j = \ell - 1$, then $\nu_\ell(k + j\ell^i) = \nu_\ell(k)$. On the other hand if $k = \ell^i$ and $j = \ell - 1$ then $\nu_\ell(k + j\ell^i) = \nu_\ell(\ell^{i+1}) = \nu_\ell(\ell^i) + 1$. We infer from (28) that

$$h(e\ell^{i+1}) = \underbrace{h(e\ell^i) + h(e\ell^i) + \cdots + h(e\ell^i)}_{\ell} + 1 = \ell s_i + 1 = s_{i+1}.$$

11.4 Lemma Let $a = ex$, where $x = b\ell^i + y$, $0 \leq i$, $0 \leq b < \ell$ and $0 \leq y < \ell^i$. Then

$$h(a) = bh(e\ell^i) + h(ey).$$

Proof. We have $a = eb\ell^i + ey$, where by (29)

$$h(a) = h(e\ell^i) + \sum_{1 \leq k \leq \ell^i} g(e(k + \ell^i)) + \cdots + \sum_{1 \leq k \leq \ell^i} g(e(k + (b-1)\ell^i)) + \sum_{1 \leq k \leq y} g(e(k + b\ell^i)).$$

If $1 \leq k \leq \ell^i$ and $0 \leq j < b$, or if $1 \leq k < \ell^i$ and $j = b$, then $\nu_\ell(k + j\ell^i) = \nu_\ell(k)$. The rest follows much as above.

11.5 Lemma If $1 \leq a \leq n$ and $\Delta(a) = (y_{-1}, y_0, \dots, y_m)$ is as given in Section 4 then

$$h(a) = y_m h(e\ell^m) + \cdots + y_1 h(e\ell) + y_0 h(e) = y_m s_m + \cdots + y_1 s_1 + y_0 s_0.$$

Proof. This follows by using Lemmas 11.3 and 11.4, as well as (29).

12 Appendix C

Here we determine when the map $P \mapsto \nu_\ell([G : P])$ is injective on \mathcal{P}^* , i.e. when $|\mathcal{P}^*(c)| = 1$ for all \mathcal{P} -values c . We adopt all of the notation introduced in Section 6. Clearly, the injectivity of ϑ on \mathcal{P}^* is equivalent to the injectivity of ϕ on \mathcal{P}^* .

We define $\check{\mathcal{P}}$ to be the set of all $[z_0, z_1, 0, \dots, 0] \in \mathcal{P}^*$. Note that $\check{\mathcal{P}} = \mathcal{P}^*$ if $\lfloor n/e \rfloor < \ell^2$.

12.1 Lemma ϕ is injective on $\check{\mathcal{P}}$ if and only if $\lfloor n/e \rfloor \leq d\ell$.

Proof. Suppose $\lfloor n/e \rfloor \leq d\ell$ and $\phi([z_0, z_1, 0, \dots, 0]) = \phi([z'_0, z'_1, 0, \dots, 0])$. By Theorem 4.3

$$z_0d + z_1(d\ell + 1) = z'_0d + z'_1(d\ell + 1).$$

Since $\gcd(d, d\ell + 1) = 1$ there must be an integer k such that

$$(z'_0, z'_1) = (z_0 + k(d\ell + 1), z_1 - kd). \quad (30)$$

Now $\lfloor n/e \rfloor \leq d\ell$ forces $0 \leq z_0, z'_0 \leq d\ell$, so (30) implies $z'_0 = z_0$, and a fortiori $z'_1 = z_1$.

Suppose next $\lfloor n/e \rfloor \geq d\ell + 1$. Then $P = [d\ell + 1, 0, \dots, 0], Q = [0, d, 0, \dots, 0] \in \check{\mathcal{P}}$ and

$$\phi(P) = (d\ell + 1)d = \phi(Q)$$

by Theorem 4.3, so ϕ is not injective on $\check{\mathcal{P}}$.

12.2 Lemma If $\lfloor n/e \rfloor \geq \ell^2 + \ell$ then ϕ is not injective on \mathcal{P}^* .

Proof. Let $P = [\ell, 0, 1, 0, \dots, 0]$ and $Q = [0, \ell + 1, 0, \dots, 0]$. Then $P, Q \in \mathcal{P}^*$ and

$$\phi(P) = d\ell + \ell(d\ell + 1) + 1 = d\ell(1 + \ell) + 1 + \ell = (1 + \ell)(d\ell + 1) = \phi(Q).$$

12.3 Lemma Suppose that $\ell^2 \leq \lfloor n/e \rfloor < \ell^2 + \ell$ and $\lfloor n/e \rfloor \leq \ell d$. Then there are no parabolic subgroups $P = [z_0, z_1, 0, \dots, 0] \in \check{\mathcal{P}}$ and $Q = [a, 0, 1, 0, \dots, 0] \in \mathcal{P}^*$ such that $\phi(P) = \phi(Q)$, except only if $d = \ell + 1$ and $\ell^2 + 1 \leq \lfloor n/e \rfloor$, when such P and Q do exist.

Proof. Suppose $\phi(P) = \phi(Q)$ for P, Q as stated. Then by Theorem 4.3

$$z_0d + z_1(d\ell + 1) = ad + \ell(d\ell + 1) + 1. \quad (31)$$

Hence there is an integer k such that

$$z_0 = a - \ell + k(d\ell + 1), \quad z_1 = 1 + \ell - kd. \quad (32)$$

If $k \leq 0$ then $1 + \ell - dk \geq 1 + \ell$, against the fact that $\lfloor n/e \rfloor < \ell(\ell + 1)$. Therefore $k > 0$.

Observe now that our hypotheses imply $\ell \leq d$. If $k \geq 3$ then $1 + \ell - kd < 0$, which is impossible. If $k = 2$ then $1 + \ell - 2d \geq 0$ implies $d = 1 = \ell$, which is absurd. The only possibility is $k = 1$ with $d = \ell$ or $d = \ell + 1$.

If $d = \ell$ our hypotheses yield $\lfloor n/e \rfloor = \ell^2$. Then from $Q = [a, 0, 1, 0, \dots, 0] \in \mathcal{P}^*$ we infer $a = 0$. Replacing the values $k = 1$, $a = 0$ and $d = \ell$ in (32) gives $z_0 = \ell^2 - \ell + 1$ and $z_1 = 1$. Then $z_0 + z_1\ell = \ell^2 - \ell + 1 + \ell = \ell^2 + 1$, contradicting the fact that $\lfloor n/e \rfloor = \ell^2$.

All in all, we must have $k = 1$ and $d = \ell + 1$. Going back to (32) we obtain $z_1 = 0$ and $z_0 = \ell^2 + 1 + a$. In particular $\lfloor n/e \rfloor \geq \ell^2 + 1$. This shows that no such P, Q exist, except when $d = \ell + 1$ and $\ell^2 + 1 \leq \lfloor n/e \rfloor < \ell^2 + \ell$. In this last case, setting $k = 1$, $a = 0$ yields $P = [\ell^2 + 1, 0, \dots, 0] \in \check{\mathcal{P}}$ and $Q = [0, 0, 1, 0, \dots, 0] \in \mathcal{P}$, with $\phi(P) = (\ell + 1)(\ell^2 + 1) = \phi(Q)$. The simplest example occurs when $\ell = 2$, $q = 7$ and $n = 10$.

- 12.4 Lemma** (a) Suppose $d \leq \ell$. Then ϑ is injective on \mathcal{P}^* if and only if $\lfloor n/e \rfloor \leq d\ell$.
(b) Suppose $d = \ell + 1$. Then ϑ is injective on \mathcal{P}^* if and only if $\lfloor n/e \rfloor \leq \ell^2$.
(c) Suppose $d > \ell + 1$. Then ϑ is injective on \mathcal{P}^* if and only if $\lfloor n/e \rfloor < \ell^2 + \ell$.

Proof. This follows from Lemmas 12.1, 12.2 and 12.3.

12.5 Example We examine the first case lying outside of the scope of Theorem 8.1, namely the case $\lfloor n/e \rfloor = d\ell + 1$ and $d \leq \ell$.

Suppose first $d < \ell$. Then $\mathcal{P}^* = \check{\mathcal{P}}$. The proof of Lemma 12.1 shows that ϕ only repeats at $P = [d\ell + 1, 0]$ and $Q = [0, d]$, so $V = |\mathcal{P}^*| - 1$. The proof of Theorem 6.3 shows that $\phi(P)$ is the $(d + 1)$ th largest value of ϕ . By Corollary 4.7 all factors of (13) are irreducible, except perhaps for the $(d + 1)$ th factor from the top, namely $M(P)$. Since ϕ only repeats at P and Q , it follows from Theorem 4.6 that either $M(P)$ is irreducible, or $M(P) = N(P) \oplus N(Q)$ with $N(P)$ and $N(Q)$ irreducible. In the latter case $c(L) = V$ and in the former $c(L) = V - 1$. Here $V = \ell d^2/2 + \ell d/2 + 2d + 1$ by Theorem 6.3 (else use $V = |\mathcal{P}^*| - 1$ and Lemma 8.4). The simplest case occurs when $\ell = 2$, $q = 5$ and $n = 6$.

Suppose next $d = \ell$. We then have $\mathcal{P}^* = \check{\mathcal{P}} \cup \{[0, 0, 1], [1, 0, 1]\}$. The proofs of Lemmas 12.1 and Lemma 12.3 show that that ϕ only repeats at $P = [\ell^2 + 1, 0, 0]$ and $Q = [0, \ell, 0]$, as well as $P' = [\ell^2 - \ell + 1, 1, 0]$ and $Q' = [0, 0, 1]$. Thus $V = |\mathcal{P}^*| - 2$. The proof of Theorem 6.3 shows that $\phi(P')$ and $\phi(P)$ are the $(\ell + 1)$ th and $(\ell + 2)$ th largest values of ϕ . The rest follows as before, except that now there are two doubtful irreducible factors, namely

$M(P')$ and $M(P)$, which are the $(\ell + 1)$ th and $(\ell + 2)$ th factors from the top. Moreover, $V = \ell^3/2 + \ell^2/2 + 2\ell + 2$. The simplest example occurs when $\ell = 2$, $q = 3$ and $n = 10$.

Acknowledgments

I want to express my deep gratitude to Professor Dragomir Djokovic for his invaluable contribution interpreting James' work, the profitable time spent together discussing Gow's conjecture, and his careful reading of the paper. I also thank Professor Rod Gow for his constant encouragement to pursue this problem. I am indebted to the referee for valuable suggestions. I am very thankful to Malena, Federico and Cecilia for their continuous help and support while this research took place.

References

- [1] B. Ackermann, *On the Loewy series of the Steinberg-PIM of finite general linear groups*, thesis, Universität Stuttgart, 2004.
- [2] G. James, *Representations of general linear groups*, London Mathematical Society Lecture Note Series, 94, Cambridge University Press, 1984.
- [3] G. James, *The decomposition matrices of $GL_n(q)$ for $n \leq n$* , Proc. London Math. Soc. (3), **60** (1990) 225-265.
- [4] R. Gow, *The Steinberg lattice of a finite Chevalley group and its modular reduction*, J. London Math. Soc. (2), **67** (2003), 593-608.
- [5] R. Steinberg, *Prime power representations of finite linear groups II*, Canad. J. Math. **9** (1957), 347-351.
- [6] F. Szechtman, *Modular reduction of the Steinberg lattice of the general linear group*, J. Algebra Appl. **7** (2008), 793-807.